This is a digital copy of a book that was preserved for generations on library shelves before it was carefully scanned by Google as part of a project to make the world's books discoverable online.

It has survived long enough for the copyright to expire and the book to enter the public domain. A public domain book is one that was never subject to copyright or whose legal copyright term has expired. Whether a book is in the public domain may vary country to country. Public domain books are our gateways to the past, representing a wealth of history, culture and knowledge that's often difficult to discover.

Marks, notations and other marginalia present in the original volume will appear in this file - a reminder of this book's long journey from the publisher to a library and finally to you.

Usage guidelines

Google is proud to partner with libraries to digitize public domain materials and make them widely accessible. Public domain books belong to the public and we are merely their custodians. Nevertheless, this work is expensive, so in order to keep providing this resource, we have taken steps to prevent abuse by commercial parties, including placing technical restrictions on automated querying.

We also ask that you:

+ *Make non-commercial use of the files* We designed Google Book Search for use by individuals, and we request that you use these files for personal, non-commercial purposes.
+ *Refrain from automated querying* Do not send automated queries of any sort to Google's system: If you are conducting research on machine translation, optical character recognition or other areas where access to a large amount of text is helpful, please contact us. We encourage the use of public domain materials for these purposes and may be able to help.
+ *Maintain attribution* The Google "watermark" you see on each file is essential for informing people about this project and helping them find additional materials through Google Book Search. Please do not remove it.
+ *Keep it legal* Whatever your use, remember that you are responsible for ensuring that what you are doing is legal. Do not assume that just because we believe a book is in the public domain for users in the United States, that the work is also in the public domain for users in other countries. Whether a book is still in copyright varies from country to country, and we can't offer guidance on whether any specific use of any specific book is allowed. Please do not assume that a book's appearance in Google Book Search means it can be used in any manner anywhere in the world. Copyright infringement liability can be quite severe.

About Google Book Search

Google's mission is to organize the world's information and to make it universally accessible and useful. Google Book Search helps readers discover the world's books while helping authors and publishers reach new audiences. You can search through the full text of this book on the web at `http://books.google.com/`

PREMIER MÉMOIRE

SUR

LA THÉORIE DES NOMBRES

PAR M. F. LANDRY

LICENCIÉ ÈS SCIENCES MATHÉMATIQUES

Février 1853

BODLEIANA

DÉMONSTRATION D'UN PRINCIPE DE LEGENDRE

RELATIF AU THÉORÈME DE FERMAT

PARIS

LIBRAIRIE DE L. HACHETTE ET Cie

RUE PIERRE-SARRAZIN, N° 14

(Près de l'École de Médecine)

1853

182. h. 12

DÉMONSTRATION

D'UN PRINCIPE DE LEGENDRE

RELATIF

AU THÉORÈME DE FERMAT.

Dans sa *Théorie des nombres*, page 12 du second supplément, Legendre énonce ce principe :

« Il existe pour chaque valeur du nombre premier n, un nombre premier $\theta = 2Kn + 1$, tel qu'on ne peut pas satisfaire à l'équation $r' = r + 1$, r et r' étant deux résidus de puissances n^{mes} divisées par θ, et tel en même temps que n ne soit pas un de ces résidus. »

Legendre démontre ensuite que cette double condition est satisfaite par $2n+1$, toutes les fois que $2n+1$ est un nombre premier, et qu'il en est de même pour les nombres premiers de la forme $4n+1$, $8n+1$, et $16n+1$; puis il ajoute, page 16, que l'on vérifierait de la même manière que les deux conditions sont encore remplies pour le cas de $\theta = 10n+1$, et celui de $\theta = 14n+1$; mais il ne fait pas cette vérification.

Pour ne laisser aucune incertitude sur cette matière délicate, en dehors de l'autorité du maître (αὐτὸς ἔφη), nous essayons de remplir cette lacune.

Commençons par le cas de $\theta = 10n+1$.

Soit α une *racine primitive* de $x^{10} \equiv 1$ (nous conservons le signe introduit par Gauss ; quant à l'expression *racine primitive*, elle doit être entendue dans le sens proposé par Euler), on sait que les résidus des

puissances n^{mes} divisées par $10n+1$ sont représentés par les dix premières puissances de α; l'équation $r'=r+1$ prend donc la forme générale $\alpha^x \equiv \alpha^y + 1$, et, à l'aide de $\alpha^{10} \equiv 1$, et de $\alpha^5 \equiv -1$, elle pourra toujours se ramener à l'une des deux relations $\alpha^x + \alpha^y + \alpha^z \equiv 0$, $\alpha^x + \alpha^y \equiv \alpha^z$, dans lesquelles x, y, z sont des nombres pairs. Si on pose alors $\alpha^2 \equiv \beta$, β étant ainsi une racine primitive de $x^5 \equiv 1$, on obtient $\beta^x + \beta^y + \beta^z \equiv 0$, ou $\beta^x + \beta^y \equiv \beta^z$.

Je dis d'abord que ces exposants x, y, z sont différents; car si on suppose qu'ils soient égaux tous les trois, ou que deux d'entre eux seulement soient égaux, on trouve des résultats de la forme $3 \equiv 0$, $\beta^\nu \equiv 0$, $2 \equiv \pm \beta^\nu$. Or les deux premiers sont absurdes, et le troisième conduit à $2^5 \equiv \pm 1$, d'où il résulterait $33 \equiv 0$, ou $31 \equiv 0$, relations impossibles, excepté la première pour $n=1$, et la seconde pour $n=3$.

Cela posé, pour démontrer l'absurdité de la première forme $\beta^x + \beta^y + \beta^z \equiv 0$ dans tous les autres cas, il suffit de remarquer que la somme des cinq premières puissances de β étant exactement divisible par $10n+1$, si on supprime dans cette somme les trois puissances données dont le résidu est zéro, il restera une relation de la forme $\beta^t + \beta^u \equiv 0$, laquelle conduit à $2 \equiv 0$.

Examinons maintenant la seconde forme $\beta^m + \beta^n \equiv \beta^z$, dans laquelle x, y, z sont différents, ainsi que nous l'avons démontré.

Pour diminuer le nombre des hypothèses à faire, on peut toujours concevoir cette relation ramenée à la forme $1 + \beta^x \equiv \beta^z$, dans laquelle x est moindre que z; car si on avait x plus grand que z, on trouverait facilement $\beta^{5-x} + 1 \equiv \beta^{5-x+z}$, et cette nouvelle relation $1 + \beta^{x'} \equiv \beta^{z'}$ substituée à la première satisferait à la condition de x' moindre que z'.

Si maintenant on pose successivement $x=1$, $x=2$, $x=3$, seules hypothèses à faire, on aura à examiner les six relations suivantes :

$$1+\beta \equiv \beta^2,\ 1+\beta \equiv \beta^3,\ 1+\beta \equiv \beta^4,\ 1+\beta^2 \equiv \beta^3,\ 1+\beta^2 \equiv \beta^4,\ 1+\beta^3 \equiv \beta^4.$$

Multiplions les trois premières par β^2, et les trois autres par β, puis ajoutons, membre à membre, les résultats obtenus respectivement avec

les relations qui les ont fournis, nous trouverons les conséquences que voici :

$$1+\beta+\beta^2+\beta^3\equiv\beta^3+\beta^4,\quad \text{ou}\quad 2\beta^2+1\equiv 0,\quad \text{d'où}\quad 2^5\equiv -1.$$
$$1+\beta+\beta^2+\beta^3\equiv\beta^3+\beta^5,\quad \text{ou}\quad \beta+1\equiv 0,\quad \text{d'où}\quad \beta\equiv -1.$$
$$1+\beta+\beta^2+\beta^3\equiv\beta^4+\beta,\quad \text{ou}\quad 2\beta^3+1\equiv 0,\quad \text{d'où}\quad 2^5\equiv -1.$$
$$1+\beta+\beta^2+\beta^3\equiv\beta^3+\beta^4,\quad \text{ou}\quad 2\beta+1\equiv 0,\quad \text{d'où}\quad 2^5\equiv -1.$$
$$1+\beta+\beta^2+\beta^3\equiv\beta^4+\beta^5,\quad \text{ou}\quad 2\beta^4+1\equiv 0,\quad \text{d'où}\quad 2^5\equiv -1.$$
$$1+\beta+\beta^2+\beta^4\equiv\beta^4+\beta^5,\quad \text{ou}\quad \beta^2+1\equiv 0,\quad \text{d'où}\quad \beta^2\equiv -1.$$

Ces diverses conséquences aboutissent à $2\equiv 0$, ou à $33\equiv 0$, résultats absurdes, excepté $33\equiv 0$ pour $n=1$.

La première condition du principe de Legendre est donc démontrée pour les facteurs premiers de la forme $\theta=10n+1$, n étant premier et plus grand que 3.

Quant à la seconde condition que n ne soit pas résidu, on a la relation $10n+1\equiv 0$, d'où l'on déduit, en observant que, si n était résidu, on aurait $n^5\equiv\pm 1$, la condition $10^5\equiv\pm 1$. On arriverait donc à l'un des deux résultats $100001\equiv 0$, $99999\equiv 0$. Or le nombre 99999 qui est égal à $9.41.271$, n'est un multiple de $10n+1$, pour aucune valeur de n, avec la condition que n soit premier ; et pour ce qui regarde le nombre 100001 qui est égal à 11.9091, il ne saurait être un multiple de $10n+1$ que pour $n=1$, et pour $n=909$, et ce dernier nombre n'est pas premier.

Si on veut s'assurer que 9091 est premier, on observera que ce nombre provenant de $\frac{10^5+1}{10+1}$, n'admet comme facteurs premiers que des nombres de la forme $10K+1$. Il suffira donc d'essayer la division par les nombres premiers de cette forme jusqu'à $\sqrt{9091}$. Ces diviseurs sont : 11, 31, 41, 61 et 71.

Occupons-nous maintenant du cas de $\theta=14n+1$.

En supposant que α soit une racine primitive de $x^{14}\equiv 1$, l'équation $r'=r+1$ équivaut à la condition $\alpha^x+1\equiv\alpha^z$, qui, à l'aide de

$\alpha^{14} \equiv 1$ et de $\alpha^7 \equiv -1$, peut toujours être ramenée à l'une des deux formes $\alpha^x + \alpha^y + \alpha^z \equiv 0$, $\alpha^x + \alpha^y \equiv \alpha^z$, x, y, z étant des nombres pairs. Si on fait alors $\alpha^2 \equiv \beta$ (β se trouve ainsi racine primitive de $x^7 \equiv 1$), on obtient l'une des deux relations $\beta^x + \beta^y + \beta^z \equiv 0$, $\beta^x + \beta^y \equiv \beta^z$.

Je dis d'abord que ces exposants sont différents entre eux, car si on les suppose égaux, ou qu'on en suppose seulement deux égaux, on trouve des résultats absurdes comme $3 \equiv 0$, $\beta^n \equiv 0$, ou bien $2 \equiv \pm \beta^n$, lequel donne $129 \equiv 0$, ou $127 \equiv 0$; or, ces nombres 129 et 127 ne sont divisibles par aucun nombre premier de la forme $14n+1$, n étant premier, si ce n'est 129 pour $n = 3$.

Cela posé, considérons la première forme $\beta^x + \beta^y + \beta^z \equiv 0$, et désignons les exposants possibles de β dans l'ordre de leur enchaînement par x_1, x_2, $x_3 \ldots x_7$, et par x_z l'un quelconque d'entre eux, quelle que soit d'ailleurs de 1 à 7 la valeur numérique de x_1.

La relation peut avoir la forme $\beta^{x_1} + \beta^{x_2} + \beta^{x_3} \equiv 0$, et alors, si on multiplie par β^3, elle produit $\beta^{x_4} + \beta^{x_5} + \beta^{x_6} \equiv 0$, de sorte qu'en ajoutant, on arrive facilement à $\beta^{x_7} \equiv 0$. Elle peut avoir la forme $\beta^{x_1} + \beta^{x_3} + \beta^{x_5} \equiv 0$, et alors, en multipliant par β, on obtient $\beta^{x_2} + \beta^{x_4} + \beta^{x_6} \equiv 0$, lequel résultat, ajouté à l'hypothèse, conduit à $\beta^{x_7} \equiv 0$. Enfin, elle peut avoir la forme $\beta^{x_1} + \beta^{x_2} + \beta^{x_z} \equiv 0$, z étant susceptible seulement des trois valeurs 4, 5 et 6. Si on suppose $z = 5$, et qu'on multiplie par β^3, on trouvera $\beta^{x_3} + \beta^{x_4} + \beta^{x_7} \equiv 0$, ce qui aboutit de suite comme précédemment à $\beta^{x_6} \equiv 0$.

Reste donc à examiner les deux hypothèses $z = 4$, $z = 6$. La première $\beta^{x_1} + \beta^{x_2} + \beta^{x_4} \equiv 0$ conduit, étant multipliée par β^4, à la relation $\beta^{x_5} + \beta^{x_6} + \beta^{x_1} \equiv 0$; de sorte qu'en ajoutant membre à membre, on obtient $\beta^{x_1} + \beta^{x_2} + \beta^{x_4} + \beta^{x_5} + \beta^{x_6} + \beta^{x_1} \equiv 0$. Si alors on ajoute $\beta^{x_3} + \beta^{x_7}$ de part et d'autre, on trouve $\beta^{x_1} \equiv \beta^{x_3} + \beta^{x_7}$ ou $\beta^{x_2} \equiv \beta^{x_4} + \beta^{x_1}$, résultat incompatible avec $\beta^{x_1} + \beta^{x_2} + \beta^{x_4} \equiv 0$, puisqu'en ajoutant on trouverait $2\beta^{x_2} \equiv 0$. La seconde $\beta^{x_1} + \beta^{x_2} + \beta^{x_6} \equiv 0$ conduit, étant multipliée par β^2, à $\beta^{x_1} + \beta^{x_2} + \beta^{x_3} + \beta^{x_4} + \beta^{x_6} + \beta^{x_1} \equiv 0$, de sorte qu'en ajoutant de part et d'autre $\beta^{x_5} + \beta^{x_7}$, on obtient $\beta^{x_1} \equiv \beta^{x_5} + \beta^{x_7}$ ou $\beta^{x_2} \equiv \beta^{x_6} + \beta^{x_1}$, résultat incompatible avec $\beta^{x_1} + \beta^{x_2} + \beta^{x_6} \equiv 0$, puisqu'en ajoutant on trouverait $2\beta^{x_2} \equiv 0$.

Passons maintenant à la seconde forme $\beta^x + \beta^y \equiv \beta^z$, ou plutôt

$1+\beta^x \equiv \beta^z$, dans laquelle x et z sont l'un et l'autre différents de 7. On peut toujours supposer x moindre que z, car si on avait x plus grand que z, la relation pourrait être remplacée par la condition équivalente $\beta^{7-x}+1 \equiv \beta^{7-x+z}$ ou $1+\beta^{x'} \equiv \beta^{z'}$, dans laquelle x' est moindre que z'.

Cela posé, les divers cas à examiner se réduisent à quinze que nous désignerons par leurs numéros d'ordre, et dont voici le tableau :

$$1+\beta\equiv\beta^2,\ 1+\beta\equiv\beta^3,\ 1+\beta\equiv\beta^4,\ 1+\beta\equiv\beta^5,\ 1+\beta\equiv\beta^6;$$
$$1+\beta^2\equiv\beta^3,\ 1+\beta^2\equiv\beta^4,\ 1+\beta^2\equiv\beta^5,\ 1+\beta^2\equiv\beta^6;$$
$$1+\beta^3\equiv\beta^4,\ 1+\beta^3\equiv\beta^5,\ 1+\beta^3\equiv\beta^6;$$
$$1+\beta^4\equiv\beta^5,\ 1+\beta^4\equiv\beta^6;\quad 1+\beta^5\equiv\beta^6.$$

Considérons d'abord les six cas [2], [4], [14], [6], [9] et [13], savoir :

$$1+\beta\equiv\beta^2,\quad 1+\beta\equiv\beta^5,\quad 1+\beta^4\equiv\beta^6,\quad 1+\beta^2\equiv\beta^3,$$
$$1+\beta^3\equiv\beta^6,\quad 1+\beta^4\equiv\beta^5.$$

Multiplions les trois premières relations par β^2, et les trois autres par β, puis ajoutons, nous trouvons

$$1+\beta+\beta^2\equiv\beta^5,\quad \beta+\beta^2+\beta^3\equiv\beta^5,\quad 1+\beta^2+\beta^4\equiv\beta,\quad 1+\beta+\beta^3\equiv\beta^4,$$
$$\beta+\beta^3+\beta^3\equiv\beta^6,\quad 1+\beta+\beta^4\equiv\beta^6;$$

on en déduit, en multipliant la troisième par β, la dernière par β^2, et par β^3 toutes les autres, puis ajoutant et complétant la série dans le premier membre, les résultats que voici :

$$\beta+\beta^5+\beta^6\equiv 0,\quad 1+\beta+\beta^5\equiv 0,\quad \beta+\beta^3+\beta^6\equiv 0,\quad 1+\beta^4+\beta^6\equiv 0,$$
$$1+\beta^3+\beta^6\equiv 0,\quad \beta+\beta^5+\beta^6\equiv 0.$$

Or, tous ces résultats rentrent dans la forme générale $\beta^x+\beta^y+\beta^z\equiv 0$, dont nous avons démontré l'absurdité.

Considérons maintenant les trois cas [3], [11], [15], c'est-à-dire $1+\beta\equiv\beta^4$, $1+\beta^3\equiv\beta^5$, $1+\beta^6\equiv\beta^6$, conditions dont la forme géné-

rale est $1+\beta^{2x}\equiv\beta^{x}$. Si on forme les carrés, on trouve $1+2\beta^{2x}+\beta^{4x}\equiv\beta^{2x}$, ou $1+\beta^{2x}+\beta^{4x}\equiv 0$, résultat qui rentre également dans la forme $\beta^{x}+\beta^{y}+\beta^{z}\equiv 0$. On peut encore multiplier par β^{x} et ajouter, on trouve $1+\beta^{3x}\equiv 0$, d'où l'on déduirait $2\equiv 0$.

Reste donc les six cas [1], [7], [12], [5], [8] et [10], savoir :

$$1+\beta\equiv\beta^{2},\quad 1+\beta^{2}\equiv\beta^{4},\quad 1+\beta^{3}\equiv\beta^{6},\quad 1+\beta\equiv\beta^{4},\quad 1+\beta^{2}\equiv\beta^{6},$$
$$1+\beta^{3}\equiv\beta^{5}.$$

Les trois premiers sont compris dans la forme générale $1+\beta^{x}\equiv\beta^{2x}$; et les trois autres qui reviennent à $\beta^{2}+\beta\equiv 1$, $\beta^{4}+\beta^{2}\equiv 1$, $\beta^{6}+\beta^{3}\equiv 1$, ont la forme commune $\beta^{x}+\beta^{2x}\equiv 1$. La première forme donne, si on élève au carré, $1+2\beta^{x}+\beta^{2x}\equiv\beta^{4x}$, et, à cause de $1+\beta^{x}\equiv\beta^{2x}$, on trouve $2\beta^{2x}+\beta^{x}\equiv\beta^{4x}$; si alors on carre de nouveau, on obtient $4\beta^{4x}+4\beta^{3x}+\beta^{2x}\equiv\beta^{8x}$, condition qui se réduit à $4(\beta^{x}+1)\beta^{3x}\equiv\beta^{x}-\beta^{2x}$, ou $4\beta^{3x}\equiv -1$, et qui conduit définitivement à $4^{7}+1\equiv 0$. La seconde forme $\beta^{x}+\beta^{2x}\equiv 1$ donne, étant carrée, $\beta^{2x}+2\beta^{3x}+\beta^{4x}\equiv 1$, ou $2\beta^{3x}+\beta^{2x}\equiv 1$, à cause de $\beta^{4x}+\beta^{2x}\equiv\beta^{2x}$; carrant alors de nouveau, on trouve $4\beta^{6x}+4\beta^{5x}+\beta^{4x}\equiv 1$, ou $4\beta^{4x}(\beta^{x}+1)\equiv 1-\beta^{4x}$; mais l'hypothèse donne $\beta^{x}+1\equiv\beta^{2x}$, et par conséquent $1-\beta^{4x}\equiv -\beta^{x}$; donc $4\beta^{10x}\equiv -\beta^{x}$. Ainsi on arrive à $4\beta^{9x}\equiv -1$, et par suite à $4^{7}+1\equiv 0$. En conséquence, on voit que dans les six derniers cas, on est conduit au même résultat $4^{7}+1\equiv 0$, ou $16385\equiv 0$, ce qui imposerait au nombre 16385 la condition d'être un multiple de $14n+1$. Or, $16385=5.29.113$, et $14n+1$ ne saurait être aucun de ces diviseurs, n étant premier, si ce n'est pour $n=2$.

La première partie du principe de Legendre se trouve donc démontrée pour les facteurs premiers de la forme $\theta=14n+1$, n étant premier et plus grand que 3.

Pour démontrer maintenant que n n'est pas résidu relativement au facteur $14n+1$, on a $14n+1\equiv 0$, condition qui conduit à $14^{7}\equiv\pm 1$, parce que si n était résidu, on aurait $n^{7}\equiv\pm 1$. Or,

1° $14^{7}+1=105413505=3.5.7027567$, et 7027567 qui est premier, ne peut être de la forme $14n+1$ que pour $n=501969$ qui n'est pas premier;

2° $14^7 - 1 = 105413503 = 13.8108731$, et 8108731 qui est premier, ne saurait être de la forme $14n+1$ que pour $n = 579195$ qui n'est pas premier. Ainsi les résultats $4^7 \pm 1 \equiv 0$ sont absurdes, puisqu'ils ne contiennent aucun diviseur premier de la forme $14n+1$, n étant premier.

Il nous reste à dire comment on peut s'assurer que les nombres 7027567, 8108731 sont premiers. Comme ces nombres en raison de leur origine $\frac{14^7+1}{14+1}$, $\frac{14^7-1}{14-1}$, ne peuvent avoir pour facteurs premiers que des nombres de la forme $14K+1$, il suffira de rechercher leur divisibilité par les nombres premiers de cette forme jusqu'à $\sqrt{8108731}$. Les diviseurs à essayer sont au nombre de 68. C'est donc là une série d'opérations très-praticables, mais fort laborieuses, d'autant plus que pour dresser la liste de ces diviseurs, ou pour les vérifier, il faut préalablement se faire une table de nombres premiers jusqu'à 2857. Voici cette liste :

29, 43, 71, 113, 127, 197, 211, 239, 281, 337, 379, 421, 449, 463, 491, 547, 617, 631, 659, 673, 701, 743, 757, 827, 883, 911, 953, 967, 1009, 1051, 1093, 1163, 1289, 1303, 1373, 1429, 1471, 1499, 1583, 1597, 1667, 1709, 1723, 1877, 1933, 2003, 2017, 2087, 2129, 2143, 2213, 2269, 2297, 2311, 2339, 2381, 2423, 2437, 2521, 2549, 2591, 2633, 2647, 2689, 2731, 2801, 2843, 2857.

Au surplus, il n'est pas nécessaire à la démonstration du principe de Legendre, de prouver que 7027567 et 8108731 sont des nombres premiers. Ce qu'il est réellement indispensable d'établir, c'est que ces nombres n'ont aucun diviseur premier de la forme $14n+1$, n étant premier. Aussi nous n'entreprendrons pas, pour abréger le calcul précédent, de recourir aux méthodes particulières qui ont pour objet de déterminer si un nombre est premier, nous réservant d'aborder ailleurs cette matière difficile, et d'y ajouter des procédés que nous croyons nouveaux; nous proposerons de rechercher seulement ce qu'il importe de savoir. La marche qui suit nous paraît présenter quelque avantage.

Après s'être assuré que les nombres dont il s'agit, n'ont aucun diviseur de la forme $14K+1$ jusqu'à 1009, on sera certain que, s'ils ont des diviseurs de la forme $14n+1$, n étant premier, ces diviseurs ne sauraient être plus grands que $\frac{8108731}{1009}$, et qu'ainsi ils doivent être moindres que 8100. On établira donc la liste des nombres de la forme $14n+1$, pour n premier, de 1009 à 8100, c'est-à-dire de $n=73$, jusqu'à $n=587$, or, pour ce travail, il suffit d'une table de nombres premiers jusqu'à 1009 seulement, table que chacun peut au besoin se construire en quelques traits de plume. On rejettera de cette liste tous les multiples de 3 et de 5 si faciles à reconnaître à la première vue, voire même ceux de 7 et de 11, et l'on déterminera ainsi les diviseurs qu'il s'agirait d'essayer. Voici ces diviseurs.

1163, 1247, 1499, 1583, 1919, 2087, 2339, 2423, 2507, 2759, 3263, 3347, 3599, 3683, 3767, 4439, 4859, 4943, 5363, 5447, 5867, 6203, 6287, 6539, 6707, 7043, 7127, 7883, 7967, 8219.

Et, avec le soin de tenir compte des égalités qui suivent : $1247=29.43$, $1919=19.101$, $2507=23.109$, $2759=31.89$, $3263=13.251$, $3599=59.61$, $3683=29.127$, $4439=23.193$, $4859=43.113$, $5363=31.173$, $5447=13.419$, $6539=13.503$, $6707=19.353$, $7967=31.257$, la liste des diviseurs à essayer se réduira aux nombres suivants :

1163, 1499, 1583, 2087, 2339, 2423, 3347, 3767, 4943, 5867, 6203, 6287, 7043, 7127, 7883, 8219.

Cette dernière liste ne contient plus que des nombres premiers.

FIN.

Imprimerie de Ch. Lahure (ancienne maison Crapelet),
rue de Vaugirard, 9, près de l'Odéon.

DEUXIÈME MÉMOIRE

SUR

LA THÉORIE DES NOMBRES,

PAR M. F. LANDRY,

LICENCIÉ ÈS SCIENCES MATHÉMATIQUES.

Juillet 1852.

BODLEIANA BIBLIOTHECA

THÉORÈME DE FERMAT.

RECHERCHES NOUVELLES. — PREMIÈRE PARTIE. — LIVRE PREMIER.

PARIS,

LIBRAIRIE DE L. HACHETTE ET Cie,

RUE PIERRE-SARRASIN, N° 14

(Près de l'École de médecine).

1853.

THÉORÈME DE FERMAT.

RECHERCHES NOUVELLES. PREMIÈRE PARTIE.

OBJET DE LA PREMIÈRE PARTIE.

La démonstration du théorème de Fermat, ou plus généralement l'impossibilité de la relation $a^n + b^n \equiv c^n$, pour un nombre *premier* n plus grand que 2, se rattache à l'impossibilité de certaines relations de la forme $\alpha^x + \alpha^y + \alpha^z \equiv 0$, dans lesquelles α est une racine *primitive* de $x^{2k} \equiv 1$, relativement à un facteur *premier* θ de la forme $2kn + 1$. En effet, toutes les fois que cette relation est impossible, ce facteur θ doit diviser l'un des nombres a, b, c; et, comme la suite des nombres *premiers* θ, pour un nombre *premier* donné n, est infinie, si la forme $\alpha^x + \alpha^y + \alpha^z \equiv 0$ était impossible pour une infinité de facteurs appartenant à cette suite, la relation $a^n + b^n \equiv c^n$ le serait en même temps, puisque l'un au moins des nombres a, b, c admettrait une infinité de facteurs.

Nous disons que la suite des nombres *premiers* de la forme $2kn + 1$, pour un nombre *premier* donné n, est infinie; car, si elle ne l'est pas, soit Θ le plus grand de tous les facteurs de cette suite, et imaginons que A soit le produit de tous ces facteurs, y compris Θ; le nombre $A^n + 1$ ne pourra être divisible par aucun d'eux, et, puisque $\frac{A^n + 1}{A + 1}$ ne peut avoir pour diviseurs *premiers* que des nombres de la forme $2kn + 1$ (1), il fau-

(1) Les nombres de la forme $\frac{a^n + b^n}{a + b}$ (n étant *premier*), ne peuvent avoir pour diviseurs *premiers* que n et des nombres de la forme $2kn + 1$; et, pour contenir n, il faut que $a + b$ le contienne. Ce principe se démontre rigoureusement, sans qu'il soit nécessaire de sup-

dra bien qu'il en existe au moins un plus grand que Θ : la suite n'est donc pas limitée.

Or nous avons fait voir, dans notre premier mémoire, que, pour $\theta = 10n + 1$, et pour $\theta = 14n + 1$, la relation $\alpha^x + \alpha^y + \alpha^z \equiv 0$ se ramène à l'une des deux formes $\varepsilon^x + \varepsilon^y + \varepsilon^z \equiv 0$, $\varepsilon^x + \varepsilon^y \equiv \varepsilon^z$ (1), ε étant, relativement à θ, une racine (2) de $x^\varphi \equiv 1$ pour $\varphi = 5$ dans le premier cas, et pour $\varphi = 7$ dans le second ; et nous avons démontré l'impossibilité de ces deux dernières relations : il en résulte que, dans l'état actuel de la science, la relation $a^n + b^n \equiv c^n$ ne peut avoir lieu pour aucune valeur donnée de n (3), si l'un des nombres a, b, c n'est divisible par les facteurs *premiers* de la forme $2n + 1$, $4n + 1$, $8n + 1$, $16n + 1$, $10n + 1$ et $14n + 1$ (4).

Pour étendre à d'autres valeurs de θ cette condition de divisibilité, nous nous sommes aperçu qu'il existe un grand nombre de cas (5) où, θ étant un nombre *premier* de la forme $2k\varphi n + 1$, et ε une racine *primitive* de $x^\varphi \equiv 1$, la relation $\alpha^x + \alpha^y + \alpha^z \equiv 0$ peut se ramener à l'une des deux formes $\varepsilon^x + \varepsilon^y + \varepsilon^z \equiv 0$, $\varepsilon^x + \varepsilon^y \equiv \varepsilon^z$; et nous en avons conclu l'utilité qu'il y aurait à constater l'impossibilité de ces deux relations pour d'autres valeurs de φ que celles déjà connues. En restreignant la question au cas où φ est un nombre *premier*, nos recherches nous ont conduit à démontrer l'impossibilité des deux relations proposées pour $\varphi = 11$, $\varphi = 13$, $\varphi = 17$ et $\varphi = 19$; et elles nous ont fait découvrir des principes généraux et des artifices d'analyse qui rendent praticable l'examen de ces relations, même pour des valeurs de φ au delà de 19.

---

poser infinie la suite des facteurs *premiers* θ : il n'y a donc pas de *cercle vicieux*. (Voir Legendre.)

(1) Le choix de ε nous ayant paru plus heureux, nous l'avons subtitué à 6.

(2) Nous supprimerons le mot *primitive* toutes les fois que φ sera *premier*, parce que, dans ce cas, les φ racines de $x^\varphi \equiv 1$ sont *primitives*. Observons, à ce sujet, que les φ premières puissances de chacune de ces racines donnant toutes les autres, on peut toujours poser : $\varepsilon \equiv \varepsilon'^{\prime}$; $\varepsilon^n \equiv \varepsilon'$; $\varepsilon^n \equiv \varepsilon'^{\prime}$, ε' étant une autre racine de $x^\varphi \equiv 1$.

(3) Nous supposons toujours que n est un nombre *premier* plus grand que 2.

(4) Voyez sur ce point, le second supplément de la *Théorie des nombres* de Legendre.

(5) Ce sera l'objet de la seconde partie de nos recherches.

PREMIER LIVRE.

Principes ayant pour objet de réduire le nombre des cas d'examen, auxquels il faut soumettre les deux relations $\varepsilon^x + \varepsilon^y + \varepsilon^z \equiv 0$, $\varepsilon^x + \varepsilon^y \equiv \varepsilon^z$, pour en démontrer l'impossibilité, φ étant un nombre *premier* quelconque (1).

PREMIER PRINCIPE.

Les deux relations $\varepsilon^x + \varepsilon^y + \varepsilon^z \equiv 0$, $\varepsilon^x + \varepsilon^y \equiv \varepsilon^z$, quand elles ne sont pas déjà de la forme $1 + \varepsilon + \varepsilon^2 \equiv 0$, $1 + \varepsilon \equiv \varepsilon^2$, peuvent être ramenées à cette forme.

Après avoir divisé par ε^y les deux relations proposées, et les avoir mises sous la forme $1 + \varepsilon^x + \varepsilon^z \equiv 0$, $1 + \varepsilon^x \equiv \varepsilon^z$, on posera $\varepsilon^x \equiv \varepsilon'$, ε' étant par cela même une autre racine de $x^\varphi \equiv 1$; puis, en déterminant m de manière à satisfaire à la condition $mx = \varphi l + 1$, on obtiendra $\varepsilon \equiv \varepsilon'^m$, et, par suite, $\varepsilon^z \equiv \varepsilon'^{mz}$, d'où l'on déduira $\varepsilon^z \equiv \varepsilon'^{z'}$, en faisant $mz = z'$: on trouvera donc, en supprimant les accents, $1 + \varepsilon + \varepsilon^2 \equiv 0$, $1 + \varepsilon \equiv \varepsilon^z$.

On voit que m dépend d'une équation indéterminée du premier degré toujours résoluble, puisque φ étant *premier* est premier avec x, un seul cas excepté, celui de $x = \varphi$ (2); ce cas conduit d'ailleurs à $2^\varphi \equiv \pm 1$, résultat dont l'impossibilité sera démontrée (3).

Comme on peut toujours supposer que z n'est pas supérieur à φ, ce

(1) C'est vraiment un siége en règle que nous entreprenons; mais la question en vaut la peine.

(2) On peut toujours supposer que x est au plus égal à φ; il ne pourrait d'ailleurs être égal à 1, puisque, dans ce cas, la transformation serait sans objet.

(3) Elle le sera dans le second livre, qui paraîtra incessamment.

premier principe réduit tout d'abord à φ le nombre des cas à examiner pour chaque relation.

DEUXIÈME PRINCIPE.

Le nombre des valeurs à essayer pour z dans chacune des relations $1 + \varepsilon + \varepsilon^z \equiv 0$, $1 + \varepsilon \equiv \varepsilon^z$ *peut être réduit à* $\frac{\varphi + 1}{2}$.

Posons $\varepsilon \equiv \varepsilon'^{\varphi - 1}$, ε' étant déterminé par la condition $\varepsilon' \equiv \varepsilon^{\varphi - 1}$, nous aurons $\varepsilon^z \equiv \varepsilon'^{\varphi - z}$, et par conséquent les relations deviendront

$$1 + \varepsilon'^{\varphi - 1} + \varepsilon'^{\varphi - z} \equiv 0, \quad 1 + \varepsilon'^{\varphi - 1} \equiv \varepsilon'^{\varphi - z};$$

de sorte qu'en divisant par $\varepsilon'^{\varphi - 1}$ on trouvera, après la suppression des accents : $1 + \varepsilon + \varepsilon^{\varphi - z + 1} \equiv 0$, $1 + \varepsilon \equiv \varepsilon^{\varphi - z + 1}$.

Réciproquement, on peut revenir de ces dernières relations aux premières ; car, si on pose $\varphi - z + 1 \equiv z'$, et qu'on ait recours au même mode de transformation, en faisant $\varepsilon \equiv \varepsilon'^{\varphi - 1}$, on trouvera $\varphi - z' + 1$ pour l'exposant de ε' dans le résultat : or, $\varphi - z' + 1$ n'est autre chose que z.

On conçoit dès lors que, si l'impossibilité est démontrée pour le cas d'un exposant particulier $\varphi - z + 1$, elle le sera en même temps pour le cas où l'exposant serait z, et réciproquement. Il suffira donc d'essayer dans les deux relations l'une des deux valeurs appartenant à chacun des groupes binaires donnés par les expressions z et $\varphi - z + 1$, en faisant varier z depuis $z = 1$ jusqu'à $z = \varphi - z + 1$, c'est-à-dire jusqu'à $z = \frac{\varphi + 1}{2}$. Ces groupes binaires sont :

$$1, \varphi; \quad 2, \varphi - 1; \quad 3, \varphi - 2; \ldots \frac{\varphi - 1}{2}, \frac{\varphi + 3}{2}; \quad \frac{\varphi + 1}{2}, \frac{\varphi + 1}{2}.$$

Le terme $\frac{\varphi + 1}{2}$ se trouvant deux fois dans le dernier groupe, le nombre des cas à examiner est réduit seulement à $\frac{\varphi + 1}{2}$.

TROISIÈME PRINCIPE.

Si on essaye pour z dans la relation $1+\varepsilon+\varepsilon^z \equiv 0$ l'une des six valeurs z', $\varphi - z' + 1$, $\frac{m\varphi+1}{z'}$, $\frac{m\varphi+z'-1}{z'}$, $\frac{m\varphi-1}{z'-1}$, $\frac{m\varphi+z'}{z'-1}$, ce seul essai dispensera d'essayer les cinq autres valeurs.

Pour arriver à ce principe, il faut remarquer d'abord que la relation $1+\varepsilon+\varepsilon^z \equiv 0$ conserve la même forme, quand on y fait l'une des suppositions suivantes :

$$\varepsilon \equiv \varepsilon'^{\varphi-1}, \text{ d'où } \varepsilon^z \equiv \varepsilon'^{\varphi-z}; \qquad \varepsilon^z \equiv \varepsilon', \text{ d'où } \varepsilon \equiv \varepsilon'^{\frac{m\varphi+1}{z}};$$

$$\varepsilon^z \equiv \varepsilon'^{\varphi-1}, \text{ d'où } \varepsilon \equiv \varepsilon'^{\frac{m\varphi-1}{z}}; \qquad \varepsilon \equiv \varepsilon'^{x}, \text{ avec } zx = m\varphi+x+1;$$

$$\varepsilon \equiv \varepsilon'^{x}, \text{ avec } zx = m\varphi+x-1.$$

Voici en effet les transformations auxquelles donnent lieu ces diverses hypothèses :

La première donne : $1+\varepsilon'^{\varphi-1}+\varepsilon'^{\varphi-z} \equiv 0$ ou $1+\varepsilon'+\varepsilon'^{\varphi-z+1} \equiv 0$;

La deuxième donne : ..... $1+\varepsilon'+\varepsilon'^{\frac{m\varphi+1}{z}} \equiv 0$;

La troisième donne : $1+\varepsilon'^{\frac{m\varphi-1}{z}}+\varepsilon'^{\varphi-1} \equiv 0$ ou $1+\varepsilon'+\varepsilon'^{\frac{m\varphi+z-1}{z}} \equiv 0$;

La quatrième donne : $1+\varepsilon'^{x}+\varepsilon'^{x+1} \equiv 0$ ou $1+\varepsilon'+\varepsilon'^{\frac{m\varphi-1}{z-1}} \equiv 0$;

La cinquième donne : $1+\varepsilon'^{x}+\varepsilon'^{x-1} \equiv 0$ ou $1+\varepsilon'+\varepsilon'^{\frac{m\varphi+z}{z-1}} \equiv 0$.

Ainsi, pour une valeur z' de z, la relation pourra être transformée de manière que l'exposant de ε prenne celle que l'on voudra des valeurs suivantes :

$$\varphi - z' + 1, \quad \frac{m\varphi+1}{z'}, \quad \frac{m\varphi+z'-1}{z'}, \quad \frac{m\varphi-1}{z'-1}, \quad \frac{m\varphi+z'}{z'-1} \text{ (1)}.$$

---

(1) m est le plus petit nombre qui rende le numérateur de chaque expression fractionnaire un multiple exact de son dénominateur. Toutes ces expressions sont moindres que φ; car, soit x la valeur de l'une d'elles, on a, pour découvrir cette valeur, une équation indéterminée du premier degré de la forme $m\varphi + a = bx$, dans laquelle a et b sont moindres que φ (le cas particulier de $z' = \varphi$ étant réservé ainsi que celui de $z' = 1$). Or on sait qu'en faisant croître x de 1 à $\varphi - 1$, on doit nécessairement trouver un produit qui, divisé par φ, donne a pour résidu.

Nous disons maintenant que, si, z' étant donné, on prend pour z l'une des valeurs déterminées par les formules précédentes, on pourra transformer $1 + \varepsilon + \varepsilon^z \equiv 0$, de manière à retrouver z' pour l'exposant de ε dans la transformée. En effet, si on fait subir à cette relation les transformations indiquées, les exposants de ε dans les transformées seront donnés par les mêmes formules

$$\varphi - z + 1, \quad \frac{m\varphi + 1}{z}, \quad \frac{m\varphi + z - 1}{z}, \quad \frac{m\varphi - 1}{z - 1}, \quad \frac{m\varphi + z}{z - 1},$$

lesquelles donnent toutes z' pour résultat, lorsqu'on substitue à z

$\varphi - z' + 1$ dans la 1re, $\frac{m\varphi + 1}{z'}$ dans la 2e, $\frac{m\varphi - 1}{z' - 1}$ dans la 3e,

$\frac{m\varphi + z' - 1}{z'}$ dans la 4e, $\frac{m\varphi + z'}{z' - 1}$ dans la 5e (1).

Ainsi il y a, dans chaque cas, une transformation qui conduit de $1 + \varepsilon + \varepsilon^z \equiv 0$, à $1 + \varepsilon' + \varepsilon'^{z'} \equiv 0$, quand on a pris pour z l'une des valeurs dont il s'agit.

En conséquence, si, z' étant donné, la relation $1 + \varepsilon + \varepsilon^z \equiv 0$ est impossible pour l'une quelconque des valeurs particulières données par les formules, elle le sera pour toutes les autres; car, quelle que soit celle de ces valeurs attribuée à z dans $1 + \varepsilon + \varepsilon^z \equiv 0$, on pourra passer de cette relation à celle-ci $1 + \varepsilon' + \varepsilon'^{z'} \equiv 0$, et de cette dernière à la relation dont l'absurdité est reconnue (2).

---

(1) Il est du reste évident que, si la relation $1 + \varepsilon' + \varepsilon'^{y} \equiv 0$ a été déduite de la relation $1 + \varepsilon + \varepsilon'^{z} \equiv 0$, en posant $\varepsilon \equiv \varepsilon'^{z}$, on doit retrouver la première, à l'aide de la seconde, en posant $\varepsilon'^{z} \equiv \varepsilon$ ou $\varepsilon' \equiv \varepsilon^{\frac{m\varphi+1}{z}}$.

(2) Cette double transformation se réduit à une seule dans l'application, parce que, si la première s'effectue en posant $\varepsilon \equiv \varepsilon'^{z}$, et la seconde en faisant $\varepsilon' \equiv \varepsilon''^{y}$, le résultat s'obtiendra tout de suite, en posant $\varepsilon \equiv \varepsilon''^{zy}$ dans la relation proposée.

QUATRIÈME PRINCIPE.

Si on essaye successivement pour z, dans chacune des relations $1+\varepsilon-\varepsilon^z\equiv 0$, $1-\varepsilon+\varepsilon^z\equiv 0$, $-1+\varepsilon+\varepsilon^z\equiv 0$, *une seule des six valeurs* z', $\varphi-z'+1$, $\frac{m\varphi+1}{z'}$, $\frac{m\varphi+z'-1}{z'}$, $\frac{m\varphi-1}{z'-1}$, $\frac{m\varphi+z'}{z'-1}$, *on sera dispensé d'essayer ces valeurs de* z *dans la relation* $1+\varepsilon\equiv\varepsilon^z$.

Les transformations opérées sur la relation $1+\varepsilon+\varepsilon^z$ peuvent l'être de la même manière sur la relation $1+\varepsilon\equiv\varepsilon^z$; seulement, comme on part de $1+\varepsilon-\varepsilon^z\equiv 0$, on arrive à trois formes distinctes, à cause des signes :

$$1+\varepsilon-\varepsilon^z\equiv 0,\quad 1-\varepsilon+\varepsilon^z\equiv 0,\quad -1+\varepsilon+\varepsilon^z\equiv 0;$$

mais il est clair qu'abstraction faite de la différence apportée par le signe, chacune des trois formes précédentes, transformée par les moyens précédemment indiqués, peut en donner cinq autres, dans lesquelles l'exposant de ε aura pour valeurs les nombres déterminés par les formules

$$\varphi-z+1,\quad \frac{m\varphi+1}{z},\quad \frac{m\varphi+z-1}{z},\quad \frac{m\varphi-1}{z-1},\quad \frac{m\varphi+z}{z-1};$$

et de plus, comme nous l'avons déjà remarqué, ces expressions donnent toutes z', lorsqu'on substitue à z

$\varphi-z'+1$ dans la 1re, $\frac{m\varphi+1}{z'}$ dans la 2e, $\frac{m\varphi-1}{z'-1}$ dans la 3e,

$\frac{m\varphi+z'-1}{z'-1}$ dans la 4e, $\frac{m\varphi+z'}{z'-1}$ dans la 5e.

Il en résulte que, si z' est l'exposant de ε dans la relation, elle pourra être transformée de manière que l'exposant de ε prenne l'une des valeurs déterminées par les formules, et que, réciproquement, si l'exposant de ε est l'une de ces valeurs, la transformation pourra reproduire z'.

En conséquence, si, z' étant donné, l'impossibilité est acquise pour les trois relations $1+\varepsilon-\varepsilon^z\equiv 0$, $1-\varepsilon+\varepsilon^z\equiv 0$, $-1+\varepsilon+\varepsilon^z\equiv 0$, z représentant l'une des valeurs déterminées par les formules, la relation

$1 + \varepsilon - \varepsilon^z \equiv 0$ le sera pour toutes les valeurs. En effet, quelle que soit celle de ces valeurs que l'on veuille considérer dans la relation $1 + \varepsilon - \varepsilon^z \equiv 0$, on pourra toujours la transformer de manière que l'exposant de ε devienne z', et une seconde transformation conduira à une relation dans laquelle l'exposant de ε sera celui pour lequel l'absurdité est acquise (1).

Nous remarquerons ici que les valeurs

$$z,\ \varphi - z + 1;\quad \frac{m\varphi + 1}{z},\ \frac{m\varphi + z - 1}{z};\quad \frac{m\varphi - 1}{z - 1},\ \frac{m\varphi + z}{z - 1},$$

forment, deux à deux, trois des groupes binaires dont il a été parlé dans le deuxième principe : en effet

$$\frac{m\varphi + 1}{z} + \frac{m\varphi + z - 1}{z} = \varphi + 1, \quad \text{en posant } m = z;$$

$$\frac{m\varphi - 1}{z - 1} + \frac{m\varphi + z}{z - 1} = \varphi + 1, \quad \text{en posant } m = z - 1;$$

donc, si l'un des deux termes d'un groupe est représenté par u, l'autre sera $\varphi - u + 1$.

Cette observation fait voir que, pour démontrer l'impossibilité de $1 + \varepsilon \equiv \varepsilon^z$, dans le cas des six valeurs dont il s'agit, on aura à choisir entre deux méthodes: celle fondée sur le deuxième principe, qui consiste à essayer pour z dans cette relation trois des six valeurs

$$z,\ \varphi - z + 1;\quad \frac{m\varphi + 1}{z},\ \frac{m\varphi + z - 1}{z};\quad \frac{m\varphi - 1}{z - 1},\ \frac{m\varphi + z}{z - 1},$$

une seule de chaque groupe; et celle qui consiste à essayer une seule de ces six valeurs dans les trois relations

$$1 + \varepsilon - \varepsilon^z \equiv 0,\quad 1 - \varepsilon + \varepsilon^z \equiv 0,\quad -1 + \varepsilon + \varepsilon^z \equiv 0.$$

---

(1) Nous avons déjà fait observer que cette double transformation se réduit à une seule.

OBSERVATIONS SUR LES FORMULES

$$z,\ \varphi - z + 1,\ \frac{m\varphi + 1}{z},\ \frac{m\varphi + z - 1}{z},\ \frac{m\varphi - 1}{z - 1},\ \frac{m\varphi + z}{z - 1}.$$

Première observation. *Les divers systèmes de valeurs, auxquels conduisent les formules, n'ont aucun terme commun.*

Les transformations indiquées dans les deux propositions précédentes, sont les seules que l'on puisse effectuer sur $1 + \varepsilon + \varepsilon^2 \equiv 0$, $1 + \varepsilon - \varepsilon^2 \equiv 0$, à cause de la condition imposée à la transformation de conserver pour ε dans la transformée deux exposants qui se suivent u, $u + 1$. En effet les hypothèses à faire sur ε, ne peuvent satisfaire à une pareille condition que de deux manières, dans la comparaison de l'un des trois termes avec l'un des deux autres : ainsi dans la comparaison du second terme avec le premier, on peut poser $\varepsilon \equiv \varepsilon'^{\varphi+1}$ ou $\varepsilon \equiv \varepsilon'^{\varphi-1}$; dans celle du troisième avec le premier, on peut poser $\varepsilon^z \equiv \varepsilon'^{\varphi+1}$ ou $\varepsilon^z \equiv \varepsilon'^{\varphi-1}$; enfin dans celle du troisième avec le second, on peut supposer $\varepsilon \equiv \varepsilon'^x$ avec $zx = m\varphi + x + 1$, ou avec $zx = m\varphi + x - 1$; mais il n'y a pas d'autres combinaisons que celles-là.

D'un autre côté, il a été établi que, z' étant donné, si l'on prend pour l'exposant de ε l'une des valeurs déterminées par les formules, on peut transformer de manière à revenir à z', et par suite à chacune des autres valeurs. Soit donc $\varepsilon \equiv \varepsilon'^x$ l'hypothèse nécessaire pour obtenir la première de ces deux transformées, puis $\varepsilon' \equiv \varepsilon''^y$ celle qu'il faut faire, en partant de celle-là, pour arriver à la seconde; il est clair qu'on parviendra directement au résultat en posant tout d'abord $\varepsilon \equiv \varepsilon''^{xy}$ dans la relation que l'on considère; et, comme cette dernière relation ne peut conserver la forme obligée que par l'une des transformations indiquées, il est évident que l'hypothèse $\varepsilon \equiv \varepsilon''^{xy}$ est nécessairement l'une de celles précédemment exposées.

Ainsi ce sont les mêmes moyens de transformation qui conduisent aux termes d'un système, en partant de l'un de ces termes; et ce sont par conséquent les mêmes formules qui expriment les diverses valeurs d'un

système en fonction de l'une quelconque de ces valeurs. En conséquence, si, après avoir obtenu un premier système de valeurs, on substitue à z dans les formules un nombre z'' différent de ceux déjà obtenus, on formera un second système de valeurs qui ne contiendra aucun terme du premier, puisque, s'il en contenait un seul, le terme commun reproduirait z'' dans le premier système.

Deuxième observation. *Si on suppose z plus grand que 2, moindre que φ, et différent de $\frac{\varphi+1}{2}$, les nombres qui composent un système seront différents entre eux, toutes les fois qu'on ne pourra pas satisfaire à la condition $z(z-1)=m\varphi-1$.*

Puisque les formules donnent les diverses valeurs d'un système à l'aide de l'une quelconque de ces valeurs, si le système contient des valeurs égales, et que l'on représente l'une d'elles par z', il y aura au moins une formule qui devra reproduire cette valeur. Il s'agit donc de voir si les égalités auxquelles conduisent les formules, quand on les égale à z', sont possibles, et dans quels cas elles le sont.

Résolvant ces égalités relativement à z', et supprimant l'accent, nous trouvons :

$$z=\frac{\varphi+1}{2},\quad (z+1)(z-1)=m\varphi,\quad z(z-1)=m\varphi-1,$$
$$z(z-1)=m\varphi-1,\quad z(z-2)=m\varphi.$$

Toutes ces conditions, à l'exception de $z(z-1)=m\varphi-1$, sont évidemment absurdes, si on suppose z plus grand que 2, moindre que φ, et différent de $\frac{\varphi+1}{2}$.

APPLICATION DES FORMULES.

Des divers systèmes de valeurs donnés par les formules.

Premier système. Le premier système se compose de deux valeurs

seulement, 1 et φ. Ce sont les seules valeurs que donnent les formules quand on y substitue 1 ou φ à z (1).

Deuxième système. Le deuxième système se compose des trois valeurs 2, $\frac{\varphi+1}{2}$, $\varphi-1$. Les formules ne donnent que ces valeurs quand on y substitue à z soit 2, soit $\frac{\varphi+1}{2}$, soit $\varphi-1$ (2).

Les nombres 3 et 4 ne feront jamais partie de ce système, à partir de $\varphi=11$; car en égalant à 3, puis à 4, les expressions $\frac{\varphi+1}{2}$ et $\varphi-1$, on trouve pour la première $\varphi=5$, $\varphi=7$, et pour la seconde $\varphi=4$, $\varphi=5$.

Troisième système. Le troisième système s'obtient en faisant $z=3$ dans les formules générales, ce qui donne :

$$3,\quad \varphi-2,\quad \frac{m\varphi+1}{3},\quad \frac{m\varphi+2}{3},\quad \frac{\varphi-1}{2},\quad \frac{m\varphi+3}{2}.$$

Ce système ne servira qu'à partir de $\varphi=7$, parce que les deux premiers systèmes donnent les valeurs relatives au cas de $\varphi=3$, et à celui de $\varphi=5$. Le nombre 3 sert à le former, parce que ce nombre ne se trouve

---

(1) Les formules donnent pour $z=1$:

$$1,\ \varphi,\ 1,\ \varphi,\quad \frac{m\varphi-1}{0},\quad \frac{m\varphi+1}{0};$$

et, pour $z=\varphi$, elles donnent :

$$\varphi,\ 1,\quad \frac{m\varphi+1}{\varphi},\quad \frac{m\varphi-1}{\varphi},\quad 1,\ \varphi.$$

L'absurdité des valeurs

$$\frac{m\varphi-1}{0},\quad \frac{m\varphi+1}{0},\quad \frac{m\varphi+1}{\varphi},\quad \frac{m\varphi-1}{\varphi},$$

se justifierait facilement, en remontant aux hypothèses qui les donnent. Les cas de $z=\varphi$ et de $z=1$ avaient du reste été réservés (page 5).

(2) On trouve

pour $z=2$: $\quad 2,\quad \varphi-1,\quad \frac{\varphi+1}{2},\quad \frac{\varphi+1}{2},\quad \varphi-1,\quad 2;$

pour $z=\frac{\varphi+1}{2}$: $\quad \frac{\varphi+1}{2},\quad \frac{\varphi+1}{2},\quad 2,\quad \varphi-1,\quad 2,\quad \varphi-1;$

pour $z=\varphi-1$: $\quad \varphi-1,\quad 2,\quad \varphi-1,\quad 2,\quad \frac{\varphi+1}{2},\quad \frac{\varphi+1}{2}.$

pas dans les deux premiers systèmes pour $\varphi = 7$, et qu'il ne s'y trouvera jamais pour aucune autre valeur de φ au delà de 7.

Les nombres obtenus pour ce système seront différents à partir de $\varphi = 11$, parce que la condition $z(z-1) = m\varphi - 1$ n'est possible pour $z = 3$, qu'en supposant $\varphi = 7$. Au delà de $\varphi = 11$ le nombre 4 ne saurait faire partie du système : on trouve en effet, en égalant à 4 les divers termes qui le composent :

$$\varphi = 6, \quad m\varphi = 11, \quad m\varphi = 10, \quad m\varphi = 9, \quad m\varphi = 5.$$

Quatrième système. Le quatrième système s'obtient en faisant $z = 4$ dans les formules, ce qui donne :

$$4, \quad \varphi, -3, \quad \frac{m\varphi + 1}{4}, \quad \frac{m\varphi + 3}{4}, \quad \frac{m\varphi - 1}{3}, \quad \frac{m\varphi + 4}{3}.$$

Ce système n'aura d'application qu'à partir de $\varphi = 13$, parce que pour $\varphi = 7$ et $\varphi = 11$, les valeurs sont données par les trois premiers systèmes. Le nombre 4 sert à le former, parce qu'il ne fait partie d'aucun des systèmes précédents, au delà de $\varphi = 11$. Les nombres obtenus pour ce système seront différents au delà de $\varphi = 13$, parce que $\varphi = 13$ est le seul cas où la condition $z(z-1) = m\varphi - 1$ puisse être satisfaite pour $z = 4$.

Enfin les systèmes suivants, s'il y a lieu de les former, s'obtiendront en substituant à z dans les formules générales l'un des nombres restant à essayer, et ainsi de suite, tant que les valeurs à essayer n'auront pas été épuisées.

Tableau des divers systèmes que l'on obtient, en donnant à φ les valeurs particulières : 3, 5, 7, 11, 13, 17 *et* 19.

Valeurs de φ.	Premier système.	Deuxième système.	Troisième système.	Quatrième système.	Cinquième. système.
$\varphi = 3$	1,3	2.			
$\varphi = 5$	1,5	2, 3, 4.			
$\varphi = 7$	1,7	2, 4, 6	3, 5.		
$\varphi = 11$	1,11	2, 6,10	3, 9, 4, 8, 5, 7.		
$\varphi = 13$	1,13	2, 7,12	3,11, 9, 5, 6, 8	4,10.	
$= 17$	1,17	2, 9,16	3,15, 6,12, 8,10	4,14,13, 5,11, 7.	
$\varphi = 19$	1,19	2,10,18	3,13,17, 7, 9,11	4,16, 5,15, 6,14	8,12.

On voit par ce tableau, qu'à l'exception des deux premiers, tous les systèmes sont complets pour $\varphi = 11$, $\varphi = 17$, c'est-à-dire lorsque $\varphi - 5$ est un multiple exact de 6; et qu'il n'y en a qu'un d'incomplet pour $\varphi = 7$, $\varphi = 13$, $\varphi = 19$, c'est-à-dire lorsque $\varphi - 5$ n'est pas un multiple de 6.

Les systèmes incomplets proviennent des valeurs égales qu'ils contiennent. Ce résultat était établi d'avance par les principes jusqu'à $\varphi = 19$; mais le fait qui les vérifie, se prolonge au delà de cette valeur. Il y a donc lieu de démontrer qu'il se continue indéfiniment.

J'observe d'abord que, lorsqu'il y a des valeurs égales, les six valeurs du système se réduisent à deux nombres distincts; trois sont égales au premier de ces nombres, et les trois autres au second. En effet, en démontrant la condition des valeurs égales, nous avons vu qu'il y avait deux formules, la quatrième et la cinquième, qui donnaient la même condition $z(z-1) = m\varphi - 1$; ainsi, dans le cas où cette condition est satisfaite, il y a trois termes égaux. Mais, si on représente par u_1, u_4, u_5 ces trois termes, eu égard au rang qu'ils occupent dans le système, les trois autres termes u_2, u_3, u_6 en raison de la remarque qui a été faite (page 10), donnent $u_2 = \varphi - u_1 + 1$, $u_3 = \varphi - u_4 + 1$, $u_6 = \varphi - u_5 + 1$; donc, à cause de $u_1 = u_4 = u_5$, on aura : $u_2 = u_3 = u_6$. Cette proposition fait voir que, si on peut satisfaire à la condition $z(z-1) = m\varphi - 1$, pour une valeur de z moindre que φ, il y aura une seconde valeur de z moindre que φ qui satisfera à la même condition.

Nous disons maintenant qu'il ne peut y avoir plus de deux valeurs de z moindres que φ, satisfaisant à la condition proposée. En effet, de $z(z-1) = m\varphi - 1$, on déduit $m = \frac{z(z-1)+1}{\varphi}$; donc m est moindre que $\frac{\varphi(\varphi-1)+1}{\varphi}$, et, *à fortiori*, il est moindre que $\varphi - 1$. Cela posé, résolvons l'équation relativement à z; nous trouvons

$$z = \frac{1 + \sqrt{4m\varphi - 3}}{2},$$

ce qui exige que $4m\varphi - 3$ soit un carré parfait. Soit donc $4m\varphi - 3 = k^2$; m étant moindre que $\varphi - 1$, k^2 sera moindre que $4\varphi(\varphi-1) - 3$; et, *à fortiori*,

k sera moindre que 2φ. On trouverait le même résultat pour toute autre valeur h qui satisferait à la condition $4m'\varphi - 3 = h^2$, z étant toujours moindre que φ. Or, en comparant les deux équations $4m\varphi - 3 = k^2$, $4m'\varphi - 3 = h^2$, on trouve : $4(m' - m)\varphi = (h + k)(h - k)$, ou $(m' - m)\varphi = \frac{h+k}{2} \cdot \frac{h-k}{2}$; et, comme φ ne saurait diviser $\frac{h-k}{2}$, parce que $h - k$ est moindre que 2φ, il faudra qu'il divise $\frac{h+k}{2}$; mais $h + k$ est moindre que 4φ, et par conséquent $\frac{h+k}{2}$ est moindre que 2φ : donc $h + k = 2\varphi$. Pour une troisième valeur de z moindre que φ, il faudrait qu'il existât un troisième nombre h' satisfaisant à la condition $4m''\varphi - 3 = h'^2$; et alors, en combinant cette équation avec $4m\varphi - 3 = k^2$, on serait conduit au résultat $h' + k = 2\varphi$, d'où il résulterait $h' = h$.

Il ne peut donc y avoir qu'un seul système incomplet (en exceptant toujours les deux premiers), dans la recherche des φ exposants de ε pour une valeur donnée de φ; et il y en aura nécessairement un quand $\varphi - 5$ ne sera pas un multiple de 6, puisque, en supprimant les cinq valeurs données par les deux premiers systèmes, et celles données par les systèmes complets, il reste deux exposants de ε à déterminer. Enfin il n'y en aura pas quand $\varphi - 5$ sera un multiple de 6, parce que, s'il en existait un, il ne donnerait que deux valeurs, de sorte que les quatre nombres restant à obtenir pour les exposants de ε ne pourraient être donnés que par deux autres systèmes incomplets.

Cette théorie prouve implicitement ce théorème au moins curieux : *En désignant par u un nombre moindre que $2\varphi - 1$, on peut toujours trouver deux valeurs de u qui satisfassent à la condition $4m\varphi - 3 = u^2$, lorsque φ est un nombre premier de la forme $6p + 1$; et l'on ne peut en trouver aucune, lorsque φ est de la forme $6p - 1$. Dans le premier cas, les deux valeurs sont liées par la relation $u + u' = 2\varphi$, et il ne peut y avoir que deux valeurs.*

FIN DU PREMIER LIVRE.

Paris. — Typographie de Firmin Didot frères, rue Jacob, 56.

TROISIÈME MÉMOIRE

SUR

LA THÉORIE DES NOMBRES,

PAR M. F. LANDRY,

LICENCIÉ ÈS SCIENCES MATHÉMATIQUES.

Mars 1854.

BODLEIANA BIBLIOTHECA

NOUVELLE MÉTHODE

Pour trouver les racines *primitives* de $x^{p-1} \equiv 1$, dans le cas d'un nombre *premier* p.

PARIS,

LIBRAIRIE DE L. HACHETTE ET Cie,

RUE PIERRE-SARRAZIN, N° 14.

(Près de l'École de médecine).

1854.

ERRATA DU DEUXIÈME MÉMOIRE.

PAGES.	LIGNES.	FAUTES.	CORRECTIONS.
3	4	ou plus généralement l'impossibilité	c'est-à-dire l'impossibilité
3	5	$a^n + b^n \equiv c^n$	$a^n + b^n = c^n$
3	13	$a^n + b^n \equiv c^n$	$a^n + b^n = c^n$
4	9	$a^n + b^n \equiv c^n$	$a^n + b^n = c^n$
4	14	nous nous sommes aperçu qu'il	et soupçonnant qu'il
4	17	; et nous en avons conclu l'utilité qu'il y aurait à	, nous avons songé à
4	29	les φ racines de $x^\varphi \equiv 1$ sont *primitives.*	les φ racines de $x^\varphi \equiv 1$ sont *primitives,* excepté 1.
5	17	celui de $x = \varphi$ (2);	celui de $x = \varphi$ ou de $x = 0$ (2);
12	8	φ, et diffèrent de	$\varphi - 1$, et diffèrent de
12	22	moindre que φ, et	moindre que $\varphi - 1$, et
13	22	avaient été réservés (page 5)	avaient été réservés (page 7)
14	11	$4, \varphi, -3,$	$4, \varphi - 3,$
14	32	$= 17$	$\varphi = 17$

Très-incessamment le deuxième livre des *Recherches nouvelles sur le théorème de Fermat.*

RACINES PRIMITIVES

De $x^{p-1} \equiv 1$ relativement à p, dans le cas d'un nombre *premier* p (*).

Euler, qui s'est beaucoup occupé des racines *primitives*, avoue, dans ses opuscules analytiques (tome premier, page 152), qu'il lui semble extrêmement difficile d'assigner ces nombres, et que leur nature doit être rangée dans les points les plus épineux de la théorie des nombres. Gauss, qui rapporte cette opinion d'Euler (*Recherches arithmétiques*, page 53 de la traduction publiée par Poullet-Deslile en 1807), propose une méthode d'une grande simplicité, mais dont l'application n'est pas sans inconvénient, quant à la longueur des calculs. Enfin M. Cauchy a démontré que les racines *primitives* relatives à un nombre *premier* p se confondent et coïncident avec les racines de certaines relations ou *équivalences*, d'un degré en x égal au nombre de ces racines (*Exercices mathématiques*, 4e année, pages 231 et 236) : ainsi les quatre racines *primitives* de $x^{p-1} \equiv 1$, relativement à $p = 13$, sont les racines de l'*équivalence* $x^4 - x^2 + 1 \equiv 0$. Ces relations s'obtiennent avec facilité pour certaines valeurs de p, mais leur formation est souvent laborieuse, et de plus il resterait à les résoudre. Il ne nous a donc pas paru que cet ingénieux théorème pût servir de base à la recherche dont il s'agit.

Nous nous décidons à faire connaître, pour la détermination de ces nombres, un procédé qui nous paraît simplifier cette recherche; mais, comme on pourrait désirer savoir comment Gauss a résolu la question, pour éviter au lecteur la peine de recourir à des ouvrages que tout le monde n'a pas sous la main, nous commencerons par exposer la méthode de cet auteur.

(*) Le cas où p n'est pas *premier*, se rattache à des questions que nous élaborons en ce moment, et sera examiné ailleurs.

Méthode de Gauss pour déterminer, relativement au nombre *premier* p, les racines *primitives* de $x^{p-1} \equiv 1$.

On prendra un nombre a quelconque moindre que p, et l'on formera la suite des restes des puissances de a, jusqu'à ce que l'on trouve $a^m \equiv 1$. Si m n'est pas égal à $p-1$, a ne sera pas racine *primitive* de $x^{p-1} \equiv 1$, il sera seulement racine *primitive* de $x^m \equiv 1$, et les divers restes obtenus seront les m racines de cette relation (*).

On prendra alors un nouveau nombre b moindre que p, différent des termes de la période obtenue, et l'on cherchera les restes de ses puissances, jusqu'à ce que l'on trouve $b^n \equiv 1$. Le nombre n ne pourra être égal à m, puisque, si l'on avait $b^m \equiv 1$, b serait racine de $x^m \equiv 1$, et devrait faire partie de la période qui contient toutes ces racines. Ce nombre n ne saurait non plus être un sous-multiple de m; car, si on avait $nn' = m$, $b^n \equiv 1$ conduirait à $b^{nn'} \equiv 1$, c'est-à-dire à $b^m \equiv 1$, et b serait encore racine de $x^m \equiv 1$. Cela posé, imaginons que n soit un multiple de m, b sera racine *primitive* dans le cas particulier de $n = p-1$; et, si cela n'a pas lieu, on sera plus près du but, puisque n sera plus grand que m.

Mais, si n n'est pas un multiple de m, soit l le plus petit multiple de n et de m, l étant plus grand que m, puisque n ne divise pas ce dernier nombre. On décomposera l en deux facteurs μ et ν *premiers* entre eux, de telle sorte que μ divise m, et que ν divise n (**); puis on prendra $A \equiv a^{\frac{m}{\mu}}$, $B \equiv b^{\frac{n}{\nu}}$; et, comme il en résulte $A^\mu \equiv 1$, et $B^\nu \equiv 1$, on sera certain d'avoir $(A.B)^{\mu\nu} \equiv 1$, c'est-à-dire que $A.B$ sera racine de $x^l \equiv 1$. Il

(*) Nous croyons devoir rappeler que nous entendons par racine *primitive* de x^u relativement à p, un nombre a tel qu'on ne peut avoir $a^z \equiv 1$ pour aucune valeur de z inférieure à u.

(**) On formera μ avec les facteurs *premiers* qui divisent m sans diviser n, et ν avec ceux qui divisent n sans diviser m. Quant aux facteurs *premiers* communs, on les placera indifféremment dans μ ou dans ν, s'ils entrent à la même puissance dans m et dans n; autrement on placera dans μ ceux qui entrent à une plus haute puissance dans m, et dans ν ceux qui entrent à une plus haute puissance dans n.

faut ajouter que A.B sera racine *primitive* de cette relation. Supposons en effet, qu'on puisse avoir $(A.B)^z \equiv 1$, z étant la puisssance minimum de A.B, pour laquelle 1 est résidu. Le nombre z ne peut être qu'un diviseur de l; et, comme μ et ν sont *premiers* entre eux, il faudrait qu'il fût de la forme $\frac{\mu}{z'} \cdot \frac{\nu}{z''}$. On en conclurait par l'élévation de $(A.B)^z \equiv 1$ à la puissance z': $B^{\mu\frac{\nu}{z''}} \equiv 1$, à cause de $A^\mu \equiv 1$; ou, par l'élévation à la puissance z'': $A^{\nu\frac{\mu}{z'}} \equiv 1$, à cause de $B^\nu \equiv 1$. Or ces deux résultats deviennent $b^{\mu\frac{n}{z''}} \equiv 1$, $a^{\nu\frac{m}{z'}} \equiv 1$, et sont incompatibles, le premier avec $b^n \equiv 1$, à moins de supposer $z'' = 1$, le second avec $a^m \equiv 1$, à moins de supposer $z' = 1$. En effet z'' et z', supposés différents de 1, sont *premiers*, l'un avec μ, et l'autre avec ν, de sorte que $\mu\frac{n}{z''}$ ne saurait être un multiple de n, ni $\nu\frac{m}{z'}$ un multiple de m.

En conséquence, si l'exposant n de $b^n \equiv 1$ n'est pas un multiple de m, on pourra toujours former un nombre A.B tel que l'exposant l de la puissance *minimum* de A.B, pour laquelle 1 est résidu, soit plus grand que m. Que si $l = p - 1$, A.B sera racine *primitive;* si non, en prenant un nombre non compris dans la suite $x^l \equiv 1$, on continuera à augmenter l'exposant de la période, jusqu'à ce que cet exposant soit égal à $p - 1$.

Une fois que l'on connaît une racine *primitive* α de $x^{p-1} \equiv 1$, on obtient toutes les autres, en cherchant les restes des puissances de α dont les exposants sont *premiers* avec $p - 1$.

Nous croyons avoir rendu, avec la simplicité dont elle est susceptible, la belle méthode de Gauss ; mais on remarquera sans doute que la nécessité de déterminer tous les termes des périodes successives, jusqu'à la période finale elle-même (*), est un grave inconvénient.

La méthode que nous avons à exposer, consiste, comme celle de Gauss, à essayer une suite de nombres; mais elle n'exige pas la formation com-

---

(*) Il y a cependant un cas où il n'est pas nécessaire de développer la période finale, c'est lorsque, dans la dernière formation des nombres A.B, on a $l = p - 1$. On en verra un exemple, page 10.

plète des périodes, et conduit, en général, avec assez de rapidité, au but qu'il s'agit d'atteindre. Elle dépend de la résolution de deux questions dont la première a été résolue par Legendre (*Théorie des nombres*, page 208).

PREMIÈRE QUESTION.

Trouver, relativement à p, le résidu de $a^{\frac{p-1}{2}}$, p étant un nombre *premier* quelconque, et a un nombre quelconque non divisible par p.

Ce résidu se trouve avec une grande facilité, à l'aide des principes donnés par Legendre, principes que nous résumons ainsi qu'il suit :

Premier principe. *Si* $c = ma + c'$, *le résidu de* $c^{\frac{a-1}{2}}$ *relativement à* a, *sera celui de* $c'^{\frac{a-1}{2}}$, *quels que soient* a *et* c.

Nous croyons inutile d'insister sur un théorème aussi simple.

Deuxième principe. *Si* c *est un nombre* premier *quelconque non diviseur de* a, *et qu'on représente par* α, β, γ... *les facteurs* premiers *qui restent dans le nombre* a *après la suppression des facteurs carrés, on aura :*

$$\frac{a}{c}^{\frac{c-1}{2}} \equiv \frac{\alpha}{c}^{\frac{c-1}{2}} \cdot \frac{\beta}{c}^{\frac{c-1}{2}} \cdot \frac{\gamma}{c}^{\frac{c-2}{2}} \cdots .$$

La raison en est que la puissance $\frac{c-1}{2}$ de tout facteur carré A^2 non divisible par c, donne 1 pour résidu, puisque $(A^2)^{\frac{c-1}{2}}$ revient à A^{c-1}.

Il résulte de ce principe que, si l'on cherche relativement à p, les résidus des nombres *premiers* 2, 3, 5, 7, etc., les résidus des nombres *composés* s'en déduiront immédiatement.

Troisième principe. *Le résidu de* $2^{\frac{c-1}{2}}$ *relativement à* c *supposé* premier, *sera* 1 *ou* -1, *suivant que* c *sera de l'une des deux formes* $8n \pm 1$, *ou de l'une des deux formes* $8n \pm 3$ (Legendre, même ouvrage, page 181) (*).

(*) Ce principe fait voir que 2 ne sera jamais racine *primitive*, relativement aux nombres *premiers* de la forme $8n \pm 1$.

QUATRIÈME PRINCIPE. *Quels que soient les nombres* premiers impairs a *et* c, *s'ils ne sont pas tous deux de la forme* $4n+3$, *le résidu de* $a^{\frac{c-1}{2}}$ *relativement à* c, *sera le même que celui de* $c^{\frac{a-1}{2}}$ *relativement à* a, *et, s'ils sont tous deux de la forme* $4n+3$, *les résidus seront égaux et de signes contraires.* (Legendre, même ouvrage, pages 198 et 386) (*).

Ces principes, dont Legendre fait usage, page 209 de sa *Théorie des nombres*, conduisent, avec une rapidité presque merveilleuse, à la détermination du résidu de $a^{\frac{p-1}{2}}$ relativement à p. On peut en faire l'application aux exemples traités par cet auteur, et l'on trouvera :

$$\frac{(601)^{506}}{1013} \equiv -1\,;\ \frac{(402)^{464}}{929} \equiv 1\,;\ \frac{(1459)^{11183445}}{22366891} \equiv -1\ (^{**}).$$

Les bornes de ce mémoire nous obligent de renvoyer aux ouvrages de Legendre et de Gauss, pour la démonstration des troisième et quatrième principes.

DEUXIÈME QUESTION.

Reconnaître si un nombre a est racine *primitive* de $x^{p-1} \equiv 1$, relativement au nombre *premier* p non diviseur de a.

On cherchera, à l'aide des principes qui précèdent, le résidu de

---

(*) Cette loi, dite de *réciprocité*, a été donnée par Legendre, dès l'année 1785. Gauss, qui avait soulevé quelques objections contre la démonstration du géomètre français, est arrivé au même résultat que lui, en se fondant sur des principes tout à fait différents. Depuis lors, Legendre, non content de perfectionner à quelques égards ses premiers travaux, a mis, en 1817, sa belle découverte à l'abri de toute critique, en exposant la dernière et la plus simple des démonstrations que Gauss en avait données.

(**) Il ne paraît pas que Legendre ait songé à tirer parti de sa loi de *réciprocité*, pour la résolution des relations $x^{\frac{c-1}{2}} \equiv -1$, relativement à c (résolution des équations *symboliques* $\left(\frac{x}{c}\right) = \pm 1$, page 220). Il fait en effet dépendre la connaissance de ces racines, de celle des racines de $x^{\frac{c-1}{2}} \equiv 1$, de sorte qu'il faut d'abord découvrir toutes ces dernières, les autres ne se déterminant que par voie d'exclusion. (*Voir*, plus bas, page 16.)

$a^{\frac{p-1}{2}}$ relativement à p. Si ce résidu est 1, a ne sera pas racine *primitive* de $x^{\frac{p-1}{2}} \equiv 1$; mais, si ce résidu est -1, il peut se faire que a soit racine *primitive* de cette relation (*).

Pour s'en assurer, soient $\alpha, \beta, \gamma \ldots$ les diviseurs *premiers* impairs de $p-1$, on cherchera les résidus des puissances $a^{\frac{p-1}{2\alpha}}$, $a^{\frac{p-1}{2\beta}}$, $a^{\frac{p-1}{2\gamma}}$,... en commençant par les plus faibles de ces puissances. Cette recherche n'exige pas la formation complète de la période, et l'on peut arriver à trouver les restes qu'il s'agit de connaître, sans passer par tous les termes de la suite (**). Si l'un de ces restes est -1, il est évident que a ne sera pas racine *primitive;* mais si aucun d'eux n'est égal à -1, a sera racine *primitive.*

Pour le démontrer, supposons que a ne soit pas racine *primitive,* et que l'on ait $a^z \equiv 1$, z étant la puissance *minimum* de a, pour laquelle 1 soit résidu. Ce nombre z devant diviser $p-1$, sans diviser $\frac{p-1}{2}$, puisque de $a^z \equiv 1$ on déduirait $a^{\frac{p-1}{2}} \equiv 1$, divisera au moins l'un des nombres $\frac{p-1}{\alpha}$, $\frac{p-1}{\beta}$, $\frac{p-1}{\gamma}$,.... Supposons qu'il divise $\frac{p-1}{\alpha}$, on déduira de $a^z \equiv 1 : a^{\frac{p-1}{\alpha}} \equiv 1$, et par suite : $(a^{\frac{p-1}{2\alpha}} + 1)(a^{\frac{p-1}{2\alpha}} - 1) \equiv 0$; d'où il faudra conclure $a^{\frac{p-1}{2\alpha}} \equiv -1$, puisqu'on ne saurait avoir $a^{\frac{p-1}{2\alpha}} \equiv 1$ sans tomber en contradiction avec l'hypothèse $a^{\frac{p-1}{2}} \equiv -1$. Si donc a n'était pas racine *primitive*, il devrait donner -1 pour résidu, au moins à l'une des puissances indiquées.

Il est important d'observer que le nombre des puissances $a^{\frac{p-1}{2\alpha}}$,

---

(*) Les *équivalences* de M. Cauchy peuvent servir à cette vérification (*Voir*, plus bas, page 18).

(**) Nous donnerons plus tard, pour cette vérification, une méthode assez rapide, fondée sur la connaissance des u premiers termes de la période.

$a^{\frac{p-1}{2\beta}}$, $a^{\frac{p-1}{2\gamma}}$, ..., dont il s'agit de chercher les résidus, est égal au nombre des diviseurs *premiers* impairs de $p-1$. Lors donc que p sera de la forme 2^k+1, tout nombre a, qui donnera $a^{\frac{p-1}{2}} \equiv -1$, sera racine *primitive*. Il en sera de même si p est de la forme $2n+1$, n étant un nombre *premier* impair, puisque alors $a^{\frac{p-1}{2n}} = a$ (*), pourvu toutefois que a soit différent de $p-1$.

Détermination des racines *primitives* de $x^{p-1} \equiv 1$ relativement à p, p étant un nombre *premier* quelconque.

Tout se réduit à trouver une de ces racines, puisqu'une seule suffit pour déterminer toutes les autres.

Pour y parvenir, on essaiera successivement, à l'aide des moyens indiqués dans les deux questions précédentes, les nombres entiers 2, 3, 4, ..., jusqu'à ce que l'on en trouve un qui satisfasse aux conditions exposées dans la seconde de ces deux propositions (**).

En appliquant cette méthode aux premières valeurs de p, jusqu'à 37, on trouve que 2 est racine *primitive* relativement aux nombres 3, 5, 11, 13, 19, 29 et 37; que 3 est racine *primitive* relativement aux

---

(*) Si, au lieu de la relation $x^{p-1} \equiv 1$, il s'agissait de la relation $x^u \equiv 1$, u étant un diviseur de $p-1$, on pourrait vérifier d'une manière analogue que a est ou n'est pas racine *primitive* de cette relation, relativement à p. Seulement il y aurait deux cas à considérer, suivant que u serait pair ou impair. Dans le premier cas, il faudrait d'abord que le résidu de $a^{\frac{p-1}{2}}$ fût $+1$ si $\frac{p-1}{u}$ était pair, et -1 si $\frac{p-1}{u}$ était impair; il faudrait avoir de plus $a^{\frac{u}{2}} \equiv -1$: le reste de la méthode s'appliquerait à u comme à $p-1$. Dans le deuxième cas, il faudrait d'abord avoir $a^{\frac{p-1}{2}} \equiv 1$, puis $a^u \equiv 1$, et il resterait à examiner si 1 n'est pas résidu pour quelqu'une des puissances de a, qui sont des sous-multiples de u par ses divers facteurs *premiers*.

(**) On aurait une règle semblable pour trouver les racines primitives de $x^u \equiv 1$, relativement à p, u étant un diviseur de $p-1$. Mais il faudrait tenir compte de la note précédente.

nombres 7, 17 et 31 ; et que 5 est racine *primitive* relativement à 23 (*).

Pour les valeurs suivantes de p

41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, . . . ,

on trouve respectivement, relativement à ces nombres, les racines *primitives minima*

6 , 3, 5, 2, 2, 2, 2, 7, 5, 3, 2, 3, 5, 2,. . . .

Dans l'application de sa méthode au cas de $p = 73$, Gauss commence par essayer 2, et il trouve $2^9 \equiv 1$: il en conclut que 2 n'est pas racine *primitive*. Essayant alors 3 qui n'est pas compris dans la période $x^9 \equiv 1$, il trouve $3^{12} \equiv 1$. De $2^9 \equiv 1$, et de $3^{12} \equiv 1$, il déduit :

$$l = 36,\ \mu = 9,\ \nu = 4;\ \frac{m}{\mu} = \frac{9}{9},\ \frac{n}{\nu} = \frac{12}{4};\ A = 2,\ B = 3^3,\ A.B = 54.$$

Les puissances de 54 lui servent à former la période $x^{36} \equiv 1$; essayant alors 5 qui n'est pas compris dans cette suite, il trouve que ce dernier nombre est racine *primitive*. Observons que, si 5 eût été racine de $x^{36} \equiv -1$, sans être racine *primitive*, il eût fallu composer un nouveau nombre A'. B', à l'aide de 5 et de 54. Ce dernier seulement eût été racine *primitive*. C'est ainsi que 52, qui n'est pas compris dans la période $x^{36} \equiv 1$, donne $52^{24} \equiv 1$, et 24 n'est pas un multiple de 36. Si donc on eût essayé 52 au lieu de 5, on aurait dû prendre :

$$l = 72,\ \mu = 9,\ \nu = 8;\ \frac{m}{\mu} = 4,\ \frac{n}{\nu} = 3;\ A' = 54^4,\ B' = 52^3,\ A'.B' = 16.10 \equiv 14;$$

et on en aurait conclu que 14 est racine *primitive* de $x^{72} \equiv 1$.

La méthode que nous proposons, donne, pour le même cas de $p = 73$: $\frac{2^{36}}{73} \equiv 1$, et $\frac{3^{36}}{73} \equiv \frac{73}{3} \equiv 1$, ce qui rend inutile l'essai des nombres 2 et 3. Mais, comme $\frac{5^{36}}{73} \equiv \frac{73^2}{5} \equiv \frac{3^2}{5} \equiv -1$, il reste à savoir si $\frac{5^{\frac{36}{3}}}{73}$ ou

(*) Tous ces résultats sont connus (*Exercices mathématiques*, pages déjà citées). M. Lefébure de Fourcy, qui les donne, à la page 233 de ses *Leçons d'algèbre*, a laissé subsister une faute d'impression dans le tableau qu'il présente. Le nombre 13, qui s'y trouve parmi les racines *primitives* de 23, ne doit pas en faire partie; et 19, qui en doit faire partie, est omis.

$\frac{5^{12}}{73}$ donne -1 pour résidu; ce qui n'est pas, car on trouve $5^{12} \equiv 9$. En conséquence 5 est racine *primitive*.

Il est loisible à chacun de vérifier qu'il ne faut pas beaucoup plus de temps pour construire, par notre méthode, la table donnée plus haut jusqu'à $p = 101$, qu'il n'en faut pour appliquer la méthode de Gauss au seul cas de $p = 73$.

Si on voulait exclure, à l'avance, tous les nombres qui donnent 1 pour résidu relativement à p, afin de n'avoir à s'occuper que de ceux qui donnent -1 pour reste, on pourrait y parvenir en résolvant la relation $x^{\frac{p-1}{2}} \equiv 1$, par la méthode des carrés (Legendre, page 220). Mais, en procédant de cette manière, on est obligé de se procurer toutes ces solutions, travail assez long, bien que très-facile, à moins de ne considérer que les premières valeurs de p.

Il nous reste à présenter deux observations ayant pour objet d'atténuer la crainte que l'on pourrait concevoir, d'être entraîné, dans certains cas, à un grand nombre d'essais infructueux, même alors que p ne serait pas très-considérable.

Première observation. — Sur le nombre des valeurs qui donnent -1 pour résidu, sans être racines *primitives*.

Rappelons d'abord qu'il n'y a que $\frac{p-1}{2}$ nombres α qui donnent -1 pour résidu, que parmi eux se trouvent toutes les racines *primitives*, et qu'il y a autant de racines de cette nature qu'il y a de nombres *premiers* avec $p-1$.

Ces principes rappelés, si on cherche combien il existe de nombres moindres que $p-1$, et *premiers* avec lui, il est clair qu'il suffira de retrancher ce résultat e de $\frac{p-1}{2}$, pour savoir combien il y a de valeurs α qui donnent -1 pour résidu, sans être racines *primitives*. Soit donc $E = \frac{p-1}{2} - e$, on voit qu'on ne pourra pas faire plus de E essais, sans rencontrer une racine *primitive*. Le nombre e est donné par la formule

$e = (p-1)\left(1-\frac{1}{\lambda}\right)\left(1-\frac{1}{\mu}\right)\left(1-\frac{1}{\nu}\right)\ldots$, dans laquelle on représente par λ, μ, ν... les facteurs *premiers* de $p-1$ (*).

D'ailleurs le nombre des essais infructueux dont la limite est E, pourra toujours être diminué, si on se dispense d'essayer les restes des puissances impaires de tout nombre α qui aurait donné -1 pour résidu, et ne serait pas racine *primitive*. C'est ainsi que, si z est la puisssance *minimum* pour laquelle $\alpha^z \equiv -1$, les résidus des puissances impaires de α donneraient également -1 pour reste, étant élevés à la puissance z. Il serait donc inutile d'essayer ces différents nombres; ajoutons que, comme on commence par les plus petites valeurs de α, les résidus des puissances de ces valeurs sont faciles à obtenir.

Deuxième observation. Dans l'essai successif des nombres entiers, les nombres α qui donnent -1 pour résidu, peuvent-ils tarder beaucoup à se présenter?

Pour répondre à cette question, il suffira de considérer les nombres *premiers*, puisque, les résidus des nombres *composés* se déduisant de ceux des nombres *premiers*, aucun nombre *composé* ne pourra donner -1 pour résidu, si les nombres *premiers* qui le précèdent dans la suite, ont tous 1 pour résidu. Nous allons donc chercher les conditions imposées à p, pour que les résidus des nombres *premiers* 2, 3, 5, 7, 11 soient égaux à 1.

D'abord il est évident que p devra être de l'une des deux formes $8n \pm 1$, sans quoi le résidu de $\frac{2}{p}^{\frac{p-1}{2}}$ serait -1.

Maintenant, pour le résidu du nombre 3, on a $\frac{3}{p}^{\frac{p-1}{2}} \equiv \frac{p}{3}$, si p est de la forme $4n+1$; et l'on a $\frac{3}{p}^{\frac{p-1}{2}} \equiv -\frac{p}{3}$, si p est de la forme $4n+3$. Or, p ne pouvant être que de l'une des deux formes $3p' \pm 1$, il est évident

(*) Voyez la note troisième, page 23.

qu'on aura 1 pour résidu, lorsque p sera à la fois de la forme $4n + 1$, et de la forme $3p' + 1$; ou bien lorsqu'il sera en même temps de la forme $4n + 3$, et de la forme $3p' - 1$. Il résulte de cette simultanéité de formes imposée à p, que ce nombre devra être de l'une des deux formes $12n \pm 1$.

En conséquence, pour que 2 et 3 donnent 1 pour résidu relativement à un nombre *premier* p, il faut que p soit en même temps de l'une des deux formes $8n \pm 1$, et de l'une des deux formes $12n \pm 1$. En écartant les formes incompatibles, on trouve que p devra être de l'une des deux formes $24n \pm 1$. Les seuls nombres *premiers* de cette forme, jusqu'à 100, sont 23, 47, 71, 73 et 97.

Cherchons de même la condition imposée à p, pour que le nombre 5 donne aussi 1 pour résidu. Nous avons : $\frac{5}{p}^{\frac{p-1}{2}} \equiv \frac{p^2}{5}$; et, les formes dont p est susceptible étant $5p' \pm 1$, $5p' \pm 2$, on aura $\frac{p^2}{5} \equiv 1$ pour les deux premières, et $\frac{p^2}{5} \equiv -1$ pour les deux autres. Le nombre p devra donc avoir l'une des deux formes $5p' \pm 1$; et, comme il doit déjà être de l'une des deux formes $24n \pm 1$, il devra être de l'une des quatre formes $120n \pm 1$, $120n \pm 49$. Ainsi, jusqu'à 100, 71 est la seule valeur de p pour laquelle 2, 3 et 5 donneraient 1 pour résidu. Jusqu'à 1000, il n'y aurait pour p que les quinze valeurs suivantes :

71, 191, 239, 241, 311, 359, 409, 431, 479, 599, 601, 719, 769, 839, 911.

Cherchons encore la condition pour que le résidu de 7 soit 1. Si p n'est pas de la forme $4n + 3$, le résidu est $\frac{7}{p}^{\frac{p-1}{2}} \equiv \frac{p^3}{7}$; et, si p est de la forme $4n + 3$, le résidu sera $\frac{7}{p}^{\frac{p-1}{2}} \equiv -\frac{p^3}{7}$. Or les valeurs de p sont $7p' \pm 1$, $7p' \pm 2$, $7p' \pm 3$; et les cubes des nombres 1, 2, — 3, donnent 1 pour résidu relativement à 7 : il est donc évident que p devra être de l'une des formes $7p' + 1$, $7p' + 2$, $7p' - 3$, lorsqu'il sera différent de $4n + 3$; et qu'il devra être de l'une des formes $7p' - 1$, $7p' - 2$, $7p' + 3$, lorsqu'il sera égal à $4n + 3$. Ainsi, pour qu'aucun des nombres 2, 3, 5 et 7

ne puisse donner d'autre résidu que 1 relativement à p, il faudra que ce dernier soit simultanément de l'une des formes $120n + 1$, $120n + 49$, et de l'une des formes $7p' + 1$, $7p' + 2$, $7p' - 3$; ou bien il faudra qu'il soit en même temps de l'une des formes $120n - 1$, $120n - 49$, et de l'une des formes $7p' - 1$, $7p' - 2$, $7p' + 3$. Or on trouve que, pour satisfaire à ces conditions, p doit être de l'une des douze formes indiquées par la formule $840n \pm a$, dans laquelle a représente l'un des nombres 1, 121, 169, 289, 311, 361. Le nombre p devant être *premier*, il ne se trouve jusqu'à 1000 que les quatre nombres 311, 479, 719 et 839 qui aient la forme voulue. Jusqu'à 10000, il ne s'en trouve que 66.

Enfin, si on veut chercher la condition pour que le résidu de 11 soit égal à 1, on a : $\frac{11}{p}^{\frac{p-1}{2}} \equiv \frac{p^5}{11}$, lorsque p est de la forme $4n + 1$; et l'on a : $\frac{11}{p}^{\frac{p-1}{2}} \equiv -\frac{p^5}{11}$, dans le cas de $p = 4n + 3$. Or les formes de p sont $11p' \pm a$, a représentant l'un des nombres 1, 2, 3, 4, 5; et, comme, relativement à 11, 1 est résidu des puissances cinquièmes des nombres 1, — 2, 3, 4, 5, on voit que les formes $11p' \pm 1$, $11p' \mp 2$, $11p' \pm 3$, $11p' \pm 4$, $11p' \pm 5$, dont p est susceptible, devront être prises avec le signe supérieur, si $p = 4n + 1$; et qu'elles devront l'être avec le signe inférieur, si $p = 4n + 3$. Il restera à faire concorder ces nouvelles expressions de p avec les précédentes, et l'on trouvera que la forme générale de p devient $9240n \pm a$, dans laquelle a désigne l'une des trente valeurs particulières que voici :

1, 169, 289, 361, 479, 529, 841, 961, 1151, 1319,
1369, 1559, 1679, 1681, 1849, 2209, 2351, 2641, 2689, 2809,
2999, 3071, 3481, 3529, 3671, 3721, 3911, 4199, 4321, 4489.

On pourrait pousser plus loin cette analyse; et, en continuant seulement jusqu'au nombre *premier* suivant qui est 13, on obtiendrait pour la forme générale de p $120120n + a$, le nombre a représentant 360 valeurs particulières différentes. Les nombres *premiers* compris dans ces 360 valeurs particulières seraient donc jusqu'à 120120, les seuls pour lesquels 2, 3, 5, 7, 11 et 13 donneraient tous 1 pour résidu.

Mais, si on s'arrête à la formule $9240n \pm a$, et qu'on la développe

jusqu'à 10000, on ne trouve que 28 nombres *premiers*, dont voici la liste :

479, 1151, 1319, 1559, 2351, 2689, 2999, 3529, 3671, 3911, 4751, 4919, 5519, 5569, 5711, 6551, 6599, 7559, 7561, 7681, 8089, 8761, 8951, 9239, 9241, 9601, 9719, 9769.

Sur ces 28 nombres, il y en a 21 relativement auxquels 13 donne — 1 pour résidu, savoir :

479, 1151, 1319, 2351, 2689, 3529, 3671, 3911, 4751, 4919, 5519, 5569, 6599, 7559, 7561, 7681, 8951, 9241, 9601, 9719 et 9769.

Parmi les sept qui restent, il s'en trouve cinq pour lesquels 17 donne — 1 pour résidu, ce sont : 1559, 2999, 6551, 8089 et 8761. Enfin 19 donne — 1 pour résidu, relativement aux deux derniers 5711 et 9239.

On peut donc affirmer que, si le nombre *premier* p ne dépasse pas 10000, quelqu'un des nombres *premiers* de 2 à 19 inclusivement, sinon plusieurs, donnera, relativement à p, — 1 pour résidu.

NOTES DU TROISIÈME MÉMOIRE.

Résolution des relations $\frac{x}{p}^{\frac{p-1}{2}} \equiv \pm 1$.

La méthode que nous avons reproduite d'après Legendre, peut être employée à faire connaître si un nombre a est racine de $x^{\frac{p-1}{2}} \equiv 1$, ou de $x^{\frac{p-1}{2}} \equiv -1$; nous nous proposons, dans cette note, de déterminer *directement* toutes les solutions de l'une et de l'autre relation (*).

Prenons, pour exemples, les deux cas traités par Legendre, à la page 220 déjà citée, celui de $p = 41$, et celui de $p = 59$.

Premier exemple, $p = 41$. On a immédiatement : $\frac{2^{20}}{41} \equiv 1$, $\frac{5^{20}}{41} \equiv \frac{41^2}{5} \equiv 1, \ldots$; on a également : $\frac{3^{20}}{41} \equiv \frac{41}{3} \equiv -1$, $\frac{7^{20}}{41} \equiv \frac{41^2}{7} \equiv \frac{6^2}{7} \equiv -1, \ldots$. Ainsi 2, 4, 5, 8, 9, 10, ... sont racines de $x^{20} \equiv 1$; et 3, 6, 7, 12, 14 ..., sont racines de $x^{20} \equiv -1$.

Mais, si on cherche la racine *primitive minimum* de $x^{40} \equiv 1$, chose facile par le procédé nouveau qui en fait un jeu charmant, cette racine qui est 6, donnera toutes les solutions demandées, et pourra même donner

(*) Le procédé de Legendre consiste à former les carrés des nombres entiers, 1, 2, 3, 4 ... $\frac{p-1}{2}$. Les restes de ces puissances sont les racines de $x^{\frac{p-1}{2}} \equiv 1$, et les nombres qui ne sont pas compris dans cette suite de restes, sont les racines de $x^{\frac{p-1}{2}} \equiv -1$. Les carrés se forment d'ailleurs avec facilité, les uns des autres, par la méthode des différences.

toutes les périodes particulières qui appartiennent aux sous-multiples de 20, savoir :

$$x^{10} \equiv \pm 1, \quad x^5 \equiv \pm 1, \quad x^4 \equiv \pm 1, \quad x^2 \equiv \pm 1.$$

En effet, à cause de $6^{20} \equiv -1$, toutes les puissances impaires de 6 seront racines de $x^{20} \equiv -1$, et toutes les puissances paires seront racines de $x^{20} \equiv 1$. Les résidus des vingt premières puissances impaires, et ceux des vingt premières puissances paires seront d'ailleurs différents, puisque 6 est racine *primitive* de $x^{40} \equiv 1$. On trouve ainsi, pour les solutions de $x^{20} \equiv -1$,

6, 11, 27, 29, 19, 28, 24, 3, 26, 34, 35, 30, 14, 12, 22, 13, 17, 38, 15, 7;

et, pour les solutions de $x^{20} \equiv 1$,

36, 25, 39, 10, 32, 4, 21, 18, 33, 40, 5, 16, 2, 31, 9, 37, 20, 23, 8, 1.

Maintenant, pour les périodes $x^{10} \equiv \pm 1$, on déduirait de $6^{20} \equiv -1$: $(6^2)^{10} \equiv -1$. Les restes des dix premières puissances impaires de 6^2 seront donc les racines de $x^{10} \equiv -1$, et les restes des dix premières puissances paires du même nombre seront les racines de $x^{10} \equiv 1$. On suivrait une marche analogue pour trouver les périodes $x^5 \equiv \pm 1$, $x^4 \equiv \pm 1$, $x^2 \equiv \pm 1$.

On voit d'ailleurs que, la période complète $x^{40} \equiv 1$ contenant toutes les autres, il suffit, pour obtenir ces diverses périodes, de prendre les termes de celle-là, de deux en deux, à partir du premier et du second; de quatre en quatre, à partir du second et du quatrième; de huit en huit, à partir du quatrième et du huitième; de dix en dix, à partir du cinquième et du dixième; de vingt en vingt, à partir du dixième et du vingtième. Le premier des deux nombres qui servent de points de départ, dans ces différents cas, conduit aux périodes dont le second membre est -1; le second conduit aux périodes dont le second membre est 1. Généralement une période $x^m \equiv 1$ pourra donner, d'une manière semblable, toutes celles dont l'exposant est un sous-multiple du sien; et l'on peut remarquer aussi que, dans toute période $x^{2n} \equiv 1$, les termes de rang impair sont les solutions de $x^n \equiv -1$, et que ceux de rang pair sont les racines de $x^n \equiv 1$. Mais les périodes particulières peuvent s'obtenir *directement* par la méthode indiquée, à l'aide d'une seule

racine *primitive* de $x^{p-1} \equiv 1$, sans qu'il soit nécessaire de connaître aucune autre période.

Deuxième exemple, $p = 59$. Aussitôt que l'on se sera assuré que 2 est racine *primitive* relativement à 59, on trouvera les solutions de $x^{29} \equiv -1$, à l'aide des puissances impaires de 2, et celles de $x^{29} \equiv 1$, à l'aide des puissances paires de ce nombre.

Les premières sont : 2, 8, 32, 10, 40, 42, 50, 23, 33, 14, 56, 47, 11, 44, 58, 55, 43, 54, 39, 38, 34, 18, 13, 52, 31, 6, 24, 37 et 30.

Les secondes sont : 4, 16, 5, 20, 21, 25, 41, 46, 7, 28, 53, 35, 22, 29, 57, 51, 27, 49, 19, 17, 9, 36, 26, 45, 3, 12, 48, 15 et 1.

Ce qui revient ici à former la période complète $x^{58} \equiv 1$, et à prendre séparément les termes de rang impair, et ceux de rang pair.

DEUXIÈME NOTE.

Sur les *équivalences* de M. Cauchy. Leur *utilité* comme moyen de vérification; leur *formation*, leur *degré*.

1. Proposons-nous d'abord de faire servir les *équivalences* à vérifier si un nombre α qui donne -1 pour résidu, est racine *primitive*. Prenons, pour exemple, $p = 31$. Développons le quotient $\frac{(x^{15}+1)(x+1)}{(x^5+1)(x^3+1)}$, l'*équivalence* sera : $x^8 + x^7 - x^5 - x^4 - x^3 + x + 1 \equiv 0$. Le nombre 3 donnant -1 pour résidu, puisque $\frac{3^{15}}{31} \equiv -\frac{31}{3} \equiv -1$, il y a lieu d'essayer ce nombre; et, comme il résout l'*équivalence*, il est racine *primitive*. Le nombre 6 donne aussi -1 pour résidu, puisque $\frac{6^{15}}{31} = \frac{2^{15}}{31} \cdot \frac{3^{15}}{31} \equiv -1$; mais il ne vérifie pas l'*équivalence*, et n'est pas racine *primitive*.

Le calcul à faire sur l'*équivalence*, pour vérifier si un nombre tel que 6 est ou n'est pas racine *primitive*, peut être simplifié. En effet l'*équivalence* devient une équation, lorsqu'on lui restitue le multiple de 31

supprimé dans le second membre. Il ne s'agit donc plus que de vérifier si le nombre 6 est racine de $x^8 + x^7 - x^5 - x^4 - x^3 + x + 1 = 31m$. L'indéterminée m n'est pas un obstacle à l'application du procédé ordinaire, et la méthode conduit aux conditions suivantes :

$$31m - 1 = 6m_1;\ m_1 - 1 = 36m_2 \equiv 5m_2;\ m_2 + 1 = 6m_3;$$
$$m_3 + 1 = 6m_4;\ m_4 + 1 = 36m_5 \equiv 5m_5;\ m_5 - 1 = 6m_6;\ m_6 - 1 = 0.$$

On en déduit successivement :

$$m_6 = 1;\ m_5 = 7;\ m_4 = 34 \equiv 3;\ m_3 = 17;$$
$$m_2 = 101 \equiv 8;\ m_1 = 41 \equiv 10;\ 31m \equiv 61.$$

Or ce dernier résultat est absurde.

2. Occupons-nous maintenant de la formation des *équivalences*.

La règle générale peut être exprimée très-simplement par la formule

$$\frac{\left(x^{\frac{p-1}{2}}+1\right).\ F(x)}{\left(x^{\frac{p-1}{2\alpha}}+1\right)\left(x^{\frac{p-1}{2\beta}}+1\right)\left(x^{\frac{p-1}{2\gamma}}+1\right)\ldots}$$

, dans laquelle on représente par $\alpha, \beta, \gamma \ldots$ les diviseurs *premiers* impairs de $p - 1$, et par $F(x)$ un certain produit formé des diviseurs en x, communs à plusieurs des facteurs binômes du dénominateur.

Cette formule, démontrée dans les *Exercices mathématiques*, peut se justifier par un petit nombre de considérations que nous essayons de présenter brièvement.

On sait que, si $f(x)$ est un diviseur de $x^{p-1} - 1$, la relation $f(x) \equiv 0$ admet autant de solutions différentes, moindres que p, qu'il y a d'unités dans le degré de la fonction. Or $x^{\frac{p-1}{2}} + 1$, qui est un diviseur de $x^{p-1} - 1$, est en même temps un multiple de chacun des diviseurs binômes $x^{\frac{p-1}{2\alpha}} + 1$, $x^{\frac{p-1}{2\beta}} + 1$, $x^{\frac{p-1}{2\gamma}} + 1$, ... puisque $\frac{p-1}{2}$ est un multiple *impair* (*) de chacun des nombres $\frac{p-1}{2\alpha}$, $\frac{p-1}{2\beta}$, $\frac{p-1}{2\gamma}$, ...

(*) Qu'on nous passe cette expression, qui signifie : *par un nombre impair.*

Il est dès lors évident que la division, indiquée par la formule, fait disparaître de la relation de $x^{\frac{p-1}{2}} + 1 \equiv 0$, qui contient toutes les racines *primitives*, les solutions qui ne sont pas racines *primitives*, et qui, d'après notre théorie, sont toutes comprises dans les relations

$$x^{\frac{p-1}{2\alpha}} + 1 \equiv 0, \quad x^{\frac{p-1}{2\beta}} + 1 \equiv 0, \quad x^{\frac{p-1}{2\gamma}} + 1 \equiv 0, \ldots ;$$

mais, comme plusieurs de ces dernières relations ont des racines communes, la fonction F (x) doit être prise de manière que les facteurs communs en x qui correspondent à ces racines, soient en égal nombre dans les deux termes de l'expression (voir ci-dessous, la loi de formation des quotients successifs).

Quand on vient à faire une application de la formule dans le cas d'un seul facteur binôme, les résultats s'obtiennent aussitôt. Ainsi, pour $p = 37$, on a : $\frac{x^{18}+1}{x^6+1} = x^{12} - x^6 + 1$; mais il n'en est plus de même quand il en existe plusieurs. Pour $p = 211$, par exemple, la formule serait $\frac{(x^{105}+1)(x^7+1)(x^5+1)(x^3+1)}{(x^{35}+1)(x^{21}+1)(x^{15}+1)(x+1)}$, résultat qui serait fort long à développer, après quoi il resterait à résoudre une *équivalence* du 48ᵉ degré.

Notre méthode évite ces opérations laborieuses : ainsi, dans ce dernier exemple, pour vérifier 2 qui donne $\frac{2^{105}}{211} \equiv -1$, on trouve aussitôt :

$$2^{\frac{105}{7}} = 2^{15} \equiv 63; \quad 2^{\frac{105}{5}} = 2^{21} \equiv 23; \quad 2^{\frac{105}{3}} = 2^{35} \equiv 197;$$

et, comme aucune de ces puissances ne donne -1 pour résidu, on en conclut que 2 est racine *primitive* relativement à 211.

3. Nous ne pouvons quitter ce sujet, sans déduire du degré même de l'*équivalence* la formule qui donne le nombre des racines *primitives*.

Le théorème dépend de la loi suivant laquelle se forment les quotients successifs de $x^{\frac{p-1}{2}} + 1$ par les divers facteurs binômes.

Le premier quotient s'obtient en divisant $x^{\frac{p-1}{2}} + 1$ par $x^{\frac{p-1}{2\alpha}} + 1$;

son expression est donc $\dfrac{x^{\frac{p-1}{2}}+1}{x^{\frac{p-1}{2\alpha}}+1}$.

Pour former le deuxième, il faut d'abord retirer du second facteur binôme $x^{\frac{p-1}{2\beta}}+1$, les diviseurs qui lui sont communs avec $x^{\frac{p-1}{2\alpha}}+1$, et qui sont $x^{\frac{p-1}{2\alpha\beta}}+1$. Ce deuxième quotient se formera alors du premier $\dfrac{x^{\frac{p-1}{2}}+1}{x^{\frac{p-1}{2\alpha}}+1}$ divisé par $\dfrac{x^{\frac{p-1}{2\beta}}+1}{x^{\frac{p-1}{2\alpha\beta}}+1}$, et sera $\dfrac{\left(x^{\frac{p-1}{2}}+1\right)\left(x^{\frac{p-1}{2\alpha\beta}}+1\right)}{\left(x^{\frac{p-1}{2\alpha}}+1\right)\left(x^{\frac{p-1}{2\beta}}+1\right)}$.

Pour obtenir le troisième quotient, il faut, avant de diviser par le troisième facteur binôme $x^{\frac{p-1}{2\gamma}}+1$, supprimer dans ce dernier les facteurs qui lui sont communs avec $\left(x^{\frac{p-1}{2\alpha}}+1\right)\left(x^{\frac{p-1}{2\beta}}+1\right)$: ces facteurs communs sont $\dfrac{\left(x^{\frac{p-1}{2\alpha\gamma}}+1\right)\left(x^{\frac{p-1}{2\beta\gamma}}+1\right)}{x^{\frac{p-1}{2\alpha\beta\gamma}}+1}$. En effet, les facteurs communs à $x^{\frac{p-1}{2\gamma}}+1$ et à $x^{\frac{p-1}{2\alpha}}+1$ sont $x^{\frac{p-1}{2\alpha\gamma}}+1$, ceux qui lui sont communs avec $x^{\frac{p-1}{2\beta}}+1$ sont $x^{\frac{p-1}{2\beta\gamma}}+1$; il s'agit donc de supprimer dans $x^{\frac{p-1}{2\gamma}}+1$ les diviseurs qui lui sont communs avec $\left(x^{\frac{p-1}{2\alpha\gamma}}+1\right)\left(x^{\frac{p-1}{2\beta\gamma}}+1\right)$; et, comme, pour supprimer dans $x^{\frac{p-1}{2}}+1$ les facteurs qui lui sont communs avec $\left(x^{\frac{p-1}{2\alpha}}+1\right)\left(x^{\frac{p-1}{2\beta}}+1\right)$, on l'a divisé par $\dfrac{\left(x^{\frac{p-1}{2\alpha}}+1\right)\left(x^{\frac{p-1}{2\beta}}+1\right)}{x^{\frac{p-1}{2\alpha\beta}}+1}$, de même il faut diviser $x^{\frac{p-1}{2}}+1$ par $\dfrac{\left(x^{\frac{p-1}{2\alpha\gamma}}+1\right)\left(x^{\frac{p-1}{2\beta\gamma}}+1\right)}{x^{\frac{p-1}{2\alpha\beta\gamma}}+1}$, puisque, pour passer d'une expression à l'autre,

il n'y a qu'à remplacer $\frac{p-1}{2}$ par $\frac{p-1}{2\gamma}$. Le troisième quotient sera donc

$$\frac{\left(x^{\frac{p-1}{2}}+1\right)\left(x^{\frac{p-1}{2\alpha\beta}}+1\right)}{\left(x^{\frac{p-1}{2\alpha}}+1\right)\left(x^{\frac{p-1}{2\beta}}+1\right)} : \frac{\left(x^{\frac{p-1}{2\gamma}}+1\right)\left(x^{\frac{p-1}{2\alpha\beta\gamma}}+1\right)}{\left(x^{\frac{p-1}{2\alpha\gamma}}+1\right)\left(x^{\frac{p-1}{2\beta\gamma}}+1\right)}.$$

En conséquence, dans la formation successive des divers quotients, le dernier obtenu devient dividende, et le diviseur qui doit servir à le diviser, se forme du dividende lui-même, en y remplaçant $\frac{p-1}{2}$ par $\frac{p-1}{2\lambda}$, λ étant le diviseur *premier* impair de $p-1$ correspondant au nouveau facteur binôme que l'on considère.

Cette loi établie, le degré de chaque quotient, qui est la différence entre le degré du dividende et celui du diviseur, est facile à déterminer.

Le degré du premier quotient sera, en effet :

$$\frac{p-1}{2} - \frac{p-1}{2\alpha}, \text{ ou } \frac{p-1}{2}\left(1-\frac{1}{\alpha}\right);$$

le degré du deuxième quotient sera :

$$\frac{p-1}{2}\left(1-\frac{1}{\alpha}\right) - \frac{p-1}{2\beta}\left(1-\frac{1}{\alpha}\right), \quad \text{ou} \quad \frac{p-1}{2}\left(1-\frac{1}{\alpha}\right)\left(1-\frac{1}{\beta}\right);$$

le degré du troisième sera :

$$\frac{p-1}{2}\left(1-\frac{1}{\alpha}\right)\left(1-\frac{1}{\beta}\right) - \frac{p-1}{2\gamma}\left(1-\frac{1}{\alpha}\right)\left(1-\frac{1}{\beta}\right),$$

ou $\frac{p-1}{2}\left(1-\frac{1}{\alpha}\right)\left(1-\frac{1}{\beta}\right)\left(1-\frac{1}{\gamma}\right)$; et ainsi de suite (*).

(*) Tout ce que nous venons de dire, dans cette note sur les *équivalences*, est facile à étendre au cas de $x^u \equiv 1$, u étant un diviseur de $p-1$. Seulement, il y aura deux cas à considérer celui de u pair, et celui de u impair. Dans le premier cas, le degré de l'*équivalence* sera $\frac{u}{2}\left(1-\frac{1}{\alpha}\right)\left(1-\frac{1}{\beta}\right)\left(1-\frac{1}{\gamma}\right)\ldots$, ou $u\left(1-\frac{1}{2}\right)\left(1-\frac{1}{\alpha}\right)\left(1-\frac{1}{\beta}\right)\left(1-\frac{1}{\gamma}\right)\ldots$; dans le second, il serait $u\left(1-\frac{1}{\alpha}\right)\left(1-\frac{1}{\beta}\right)\left(1-\frac{1}{\gamma}\right)\ldots$, parce que la formule de l'*équivalence* devient $\frac{(x^u-1).\,F(x)}{\left(x^{\frac{u}{\alpha}}-1\right)\left(x^{\frac{u}{\beta}}-1\right)\left(x^{\frac{u}{\gamma}}-1\right)\ldots}$; nous désignons toujours par α, β, γ... les diviseurs *premiers* impairs de u. Or il y a autant de racines *primitives* de $x^u \equiv 1$, qu'il y a de nombres *premiers* avec u; il en résulte donc une démonstration indirecte de la formule mentionnée à la page 12, formule qui fait l'objet de la note troisième.

TROISIÈME NOTE.

Démonstration directe de la formule $N = n\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)\ldots$.

Cette formule, qui sert à déterminer combien il y a, jusqu'à n, de nombres *premiers* avec n, et dans laquelle a, b, c,... représentent ses diviseurs *premiers*, se trouve dans Gauss, page 52 de l'ouvrage cité; mais il omet de la démontrer, comme étrangère à son but, et pouvant se démontrer sans peine par la théorie des combinaisons. On la reconnaît également, bien que sous un énoncé différent, page 352 de la théorie des nombres; mais le raisonnement de Legendre nous semble beaucoup trop succinct. Enfin nous la trouvons dans les exercices de M. Cauchy, année déjà citée, page 228; mais ce géomètre la déduit comme conséquence du nombre des racines *primitives*, annonçant qu'il serait facile de la démontrer directement. Bien que cette formule résulte aussi des principes de la note précédente, nous pensons devoir en donner une démonstration directe.

Soit $n = a^{\alpha}.b^{\beta}.c^{\gamma}$, en nous bornant à trois facteurs *premiers*, ce qui n'ôte rien du reste à la généralité du raisonnement.

Il faut d'abord rejeter de la suite des nombres entiers de 1 à n, tous ceux qui sont multiples de a. Ces multiples sont :

$$a,\ 2a,\ 3a,\ldots\qquad a^{\alpha-1}.b^{\beta}.c^{\gamma}.a;$$

de sorte qu'il y en a $\frac{n}{a}$, et que par conséquent de 1 à n, il se trouve $n-\frac{n}{a}$ ou $n\left(1-\frac{1}{a}\right)$ nombres *premiers* avec a.

Il faut maintenant rejeter de la suite des nombres entiers, après le rejet des multiples de a, tous ceux des termes restant qui sont multiples de b. De 1 à n, les multiples de b sont :

$$b,\ 2b,\ 3b,\ldots\qquad a^{\alpha}.b^{\beta-1}.c^{\gamma}.b;$$

et il s'agit de savoir combien parmi ces nombres, il s'en trouve de *premiers* avec a, puisque tous ceux d'entre eux qui contiennent a, ont déjà disparu dans la suite des n premiers nombres. Pour le connaître, il suffit de considérer la suite des coefficients de b qui sont 1, 2, 3,... $a^{\alpha}.b^{\beta-1}.c^{\gamma}$. Or, dans cette suite de termes dont le nombre est $\frac{n}{b}$, il y a $\frac{n}{b}\left(1-\frac{1}{a}\right)$ nom-

bres *premiers* avec a, conformément au raisonnement qui a précédé; car ce raisonnement étant vrai pour n, est vrai pour tout autre nombre n', pourvu qu'il soit un multiple de a, et peut par conséquent s'appliquer au cas de $n' \equiv \frac{n}{b}$. Ainsi l'expression $n\left(1-\frac{1}{a}\right)-\frac{n}{b}\left(1-\frac{1}{a}\right)$, ou plus simplement $n\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)$, indique combien il y a de nombres *premiers* avec a et b, de 1 à n.

Il faut encore, après ce double rejet, retrancher des termes restant de la suite des n premiers nombres entiers, les multiples de c. De 1 à n, les multiples de c sont c, $2c$, $3c$,... $a^{\alpha}.b^{\beta}.c^{\gamma-1}.c$; mais nous ne devons prendre parmi ces multiples que ceux qui sont *premiers* avec a et b, puisque tous les autres ont déjà été écartés. Tout se réduit donc à en connaître le nombre qui est $\frac{n}{c}\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)$. En effet, les facteurs a et b ne pouvant se trouver que dans les coefficients de c, c'est-à-dire dans la suite 1, 2, 3... $\frac{n}{c}$, on peut appliquer à cette suite de 1 à $\frac{n}{c}$, le raisonnement fait pour la suite de 1 à n, et l'on obtiendra le résultat en remplaçant n par $\frac{n}{c}$ dans l'expression.

Le nombre cherché N sera donc définitivement :

$$N = n\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)-\frac{n}{c}\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right),$$

c'est-à-dire : $N = n\left(1-\frac{1}{a}\right)\left(1-\frac{1}{b}\right)\left(1-\frac{1}{c}\right)$ (*).

(*) Depuis que ce mémoire est écrit, nous nous apercevons qu'une démonstration semblable se trouve, page 310, dans l'*algèbre* de M. Cirodde, qui la donne d'après M. Poinsot. Il paraît que ce savant l'avait publiée, avec d'autres propositions, dans le dixième volume du *Journal des mathématiques* de M. Liouville. Nous ne croyons pas devoir la supprimer de ce mémoire, où sa place est marquée.

Paris. — Typographie de Firmin Didot frères, rue Jacob, 56.

QUATRIÈME MÉMOIRE

SUR

LA THÉORIE DES NOMBRES,

PAR M. F. LANDRY,

LICENCIÉ ÈS SCIENCES MATHÉMATIQUES.

Février 1855.

THÉORÈME DE FERMAT.

RECHERCHES NOUVELLES. — PREMIÈRE PARTIE. — LIVRE DEUXIÈME.

PARIS,

LIBRAIRIE DE L. HACHETTE ET Cie,

RUE PIERRE-SARRAZIN, N° 14.

(Près de l'École de médecine).

1855.

ERRATA DU TROISIÈME MÉMOIRE.

PAGES.	LIGNES.	FAUTES.	CORRECTIONS.
3	2	qui nous paraît simplifier cette recherche;	qui nous paraît en simplifier la recherche;
4	25	*primitive* de x^n	*primitive* de x^n
7	1	premiers impairs	premiers *impairs*
20	2	la relation de $x^{\frac{p-1}{2}} + 1$	la relation $x^{\frac{p-1}{2}} + 1$
21	15	diviser $x^{\frac{p-1}{2}} + 1$ par	diviser $x^{\frac{p-1}{27}} + 1$ par
24	21	dans *l'Algèbre* de M. Cirodde	dans *l'Arithmétique* de M. Cirodde
24	23	M. Liouville. Nous ne croyons pas devoir.....	M. Liouville. Enfin elle se trouve encore dans l'introduction de la *Théorie des nombres* de Legendre, pages 7 et 8. Nous ne croyons cependant pas devoir...

Le troisième et dernier livre de la première partie des *Recherches nouvelles sur le théorème de Fermat* paraîtra prochainement.

THÉORÈME DE FERMAT.

RECHERCHES NOUVELLES. PREMIÈRE PARTIE. LIVRE SECOND.

Nous avons consacré un premier livre à faire voir comment les relations de la forme $\varepsilon^x + \varepsilon^y + \varepsilon^z \equiv 0$, $\varepsilon^x + \varepsilon^y \equiv \varepsilon^z$ peuvent se ramener à la forme $1 + \varepsilon + \varepsilon^z \equiv 0$, $1 + \varepsilon \equiv \varepsilon^z$; et nous avons essayé de circonscrire le champ des examens auxquels il faut soumettre ces dernières pour en vérifier l'impossibilité. Au début de ces transformations, il nous a fallu réserver, après la division par ε^y qui conduit aux formes $1 + \varepsilon^x + \varepsilon^z \equiv 0$, $1 + \varepsilon^x \equiv \varepsilon^z$, le double cas de $x = 0$ et de $x = \varphi$, pour lesquels les relations proposées deviennent $\varepsilon^z \equiv -2$, $2 \equiv \varepsilon^z$, et donnent par conséquent $2^\varphi \equiv \pm 1$. Il va être démontré qu'un pareil résultat est généralement impossible, et qu'il ne saurait avoir lieu dans les divers cas particuliers de $\varphi = 5$, $\varphi = 7$, $\varphi = 13$, $\varphi = 17$, $\varphi = 19$, sauf à excepter un nombre déterminé de valeurs θ qui échappent à notre analyse. Ainsi, ces facteurs θ exceptés, il ne restera aucune objection au système de transformation qui sert de base à notre théorie.

Ce second livre a pour objet l'impossibilité, relativement à θ, des relations $1 + \varepsilon + \varepsilon^z \equiv 0$, $1 + \varepsilon \equiv \varepsilon^z$, pour certaines valeurs particulières de z, φ étant un nombre *premier* quelconque plus grand que 3.

Nous rappelons que, dans toutes ces propositions, n est un nombre *premier* plus grand que 2; que θ est un nombre *premier* de la forme $2k\varphi n + 1$; et que ε est une racine de $x^\varphi \equiv 1$, autre que l'unité.

PREMIER PRINCIPE.

Impossibilité des deux relations $1+\varepsilon+\varepsilon^z \equiv 0$, $1+\varepsilon \equiv \varepsilon^z$, pour $z=1$ et pour $z=\varphi$.

La relation $1+\varepsilon \equiv \varepsilon^z$ devient $1 \equiv 0$ pour $z=1$ et pour $z=\varphi$; mais la relation $1+\varepsilon+\varepsilon^z \equiv 0$ devient, pour les mêmes valeurs, $2^\varphi \equiv -1$. Il n'y a donc de difficulté que pour celle-ci, et, à cause du double cas réservé au premier principe du livre premier, page 5, nous allons examiner cette double forme $2^\varphi \equiv \pm 1$.

L'impossibilité de cette relation a été démontrée pour $\varphi=5$ et pour $\varphi=7$, aux pages 4 et 6 de notre premier mémoire. Elle n'admet aucune exception pour n plus grand que 3, et, même dans le cas de $n=3$, il n'y a d'exception que pour trois facteurs θ, savoir 31, 43 et 127.

Pour $\varphi=11$, on trouve $2048 \pm 1 \equiv 0$; or $2049=3.683$, et 683, qui est *premier* et égal à $2.11.31+1$, ne peut être de la forme $2k\varphi n+1$, à moins que l'on ait $kn=31$. Quant à 2047 qui est égal à 23.89, ses diviseurs *premiers* ne peuvent avoir la forme $2k\varphi n+1$, dans le cas de $\varphi=11$, que si on pose $kn=1$ ou $kn=4$. L'impossibilité est donc manifeste, puisque n est plus grand que 2, excepté pour un seul facteur θ, savoir 683, dans le cas $n=31$.

Pour $\varphi=13$, on trouve $8192 \pm 1 \equiv 0$; mais $8193=3.2731$, et 2731, qui est *premier*, est égal à $2.3.5.7.13+1$: il ne saurait par conséquent être de la forme $2k\varphi n+1$, pour $\varphi=13$, que si on suppose $kn=3.5.7$. Quant à 8191 qui est *premier* et égal à $2.3.3.5.7.13+1$, il ne saurait être de la forme $2k\varphi n+1$ pour $\varphi=13$, que si on suppose $kn=3.3.5.7$. L'absurdité est donc évidente pour n plus grand que 7; et, même pour chacun des cas $n=3$, $n=5$, $n=7$, il n'y a que deux facteurs θ pour lesquels l'absurdité ne se trouve pas acquise, 2731 et 8191.

Pour $\varphi=17$, on trouve $131072 \pm 1 \equiv 0$; mais 131073 est égal à 3.43691, et 43691, qui est *premier* et égal à $2.5.17.257+1$, ne saurait être de la forme $2k\varphi n+1$ pour $\varphi=17$, que si l'on a $kn=5.257$. Quant à 131071 qui est *premier*, il est égal à $2.3.5.17.257+1$: en conséquence, pour qu'il fût de la forme $2k\varphi n+1$, dans l'hypothèse de $\varphi=17$, il fau-

drait que l'on eût $kn = 3.5.257$. Ainsi, dans le cas particulier de $n = 3$, il n'existe qu'un facteur θ que l'évidence n'atteint pas, savoir 131071; dans celui de $n = 5$ et dans celui de $n = 257$, il y en a deux, 43691 et 131071.

Examinons encore le cas de $\varphi = 19$: on trouve $524288 \pm 1 \equiv 0$. Or $524289 = 3.174763$, et 174763, qui est *premier*, est égal à $2.3.3.7.19.73 + 1$, de sorte qu'il ne pourrait être de la forme $2k\varphi n + 1$ pour $\varphi = 19$, que si on supposait $kn = 3.3.7.73$. Quant à 524287 qui est *premier*, il est égal à $2.3.3.3.7.19.73 + 1$, et ne peut être de la forme $2k\varphi n + 1$ pour $\varphi = 19$, que si l'on a $kn = 3.3.3.7.73$. En conséquence, dans chacun des cas $n = 3$, $n = 7$, $n = 73$, il y a deux facteurs θ qui resteraient exceptés, 174763 et 524287 (*).

On peut continuer pour les valeurs de φ au delà de 19, et il est clair que, si, pour une valeur donnée de φ, on décompose $2^\varphi \pm 1$ en ses facteurs *premiers*, la décomposition fera connaître les quelques facteurs θ pour lesquels on ne peut rien conclure, dans le cas de certaines valeurs déterminées de n; et qu'en même temps le théorème se trouvera démontré non-seulement pour toutes les autres valeurs de n, sans exception d'aucun facteur θ, mais même pour ces valeurs déterminées de n, sauf à excepter les quelques facteurs donnés par la décomposition (**).

(*) On peut facilement procéder à la vérification des nombres *premiers* que nous avons déclarés tels, parce que les nombres de la forme $\frac{2^\varphi + 1}{2 + 1}$, et ceux de la forme $\frac{2^\varphi - 1}{2 - 1}$ n'admettent pour diviseurs *premiers* que des facteurs de la forme $2m\varphi + 1$; or il suffit d'essayer ces derniers jusqu'à la racine carrée du nombre que l'on considère. Les nombres à essayer comme diviseurs sont :

pour 683,	23;					
pour 2731,	aucun;					
pour 8191,	53,	79;				
pour 43691,	103,	137;				
pour 131071,	103,	137,	239,	307;		
pour 174763,	191,	229;				
pour 524287,	191,	229,	419,	457,	571,	647.

(**) Voir la première note, page 19.

Dans les calculs qui viennent d'être présentés, les nombres $\frac{2^\varphi+1}{2+1}-1$, $\frac{2^\varphi-1}{2-1}-1$ sont divisibles par φ. Les nombres compris dans ces formules le seront toujours, à cause de la nature des diviseurs de $\frac{2^\varphi+1}{2+1}$ et de $\frac{2^\varphi-1}{2-1}$, qui sont tous de la forme $2m\varphi+1$, de sorte que leur produit est nécessairement de la forme $2M\varphi+1$. Mais on a pu remarquer de plus que le nombre $\frac{2^\varphi-1}{2-1}-1$ est un multiple par 3 du nombre $\frac{2^\varphi+1}{2+1}-1$: c'est ce qui résulte en effet de la double égalité

$$\frac{2^\varphi-1}{2-1}-1=\frac{2(2^{\varphi-1}-1)}{2-1},\quad \frac{2^\varphi+1}{2+1}-1=\frac{2(2^{\varphi-1}-1)}{3}.$$

On voit encore que, 2 excepté, les facteurs communs à ces deux nombres sont ceux de $\frac{2^{\varphi-1}-1}{3}$. Les formes particulières, auxquelles sont soumis les diviseurs *premiers* de cette expression, feront donc facilement découvrir ces facteurs (*).

DEUXIÈME PRINCIPE.

Impossibilité des deux relations $1+\varepsilon+\varepsilon^z\equiv 0$, $1+\varepsilon\equiv\varepsilon^z$, pour $z=2$, $z=\frac{\varphi+1}{2}$, $z=\varphi-1$.

Pour la première relation $1+\varepsilon+\varepsilon^z\equiv 0$, les trois valeurs 2, $\frac{\varphi+1}{2}$, $\varphi-1$ appartiennent, suivant le troisième principe du premier livre, pages 7 et 13, à une seule et même forme $1+\varepsilon+\varepsilon^2\equiv 0$ dont l'absurdité est évidente, excepté pour $\varphi=3$, puisqu'elle donne $\varepsilon^3-1\equiv 0$.

Pour la seconde relation $1+\varepsilon\equiv\varepsilon^z$, d'après le deuxième principe du

(*) Voir la seconde note, pour la généralisation du principe, page 19.

premier livre, page 6, le cas de $z=\varphi-1$ dépend de celui de $z=2$; et, dans ce dernier cas, $1+\varepsilon\equiv\varepsilon^2$ devient aisément $\varepsilon-\varepsilon^{\varphi-1}\equiv 1$. C'est sous cette forme que nous nous proposons d'examiner la possibilité de $1+\varepsilon\equiv\varepsilon^z$ pour $z=2$ et pour $z=\varphi-1$. Quant à l'hypothèse de $z=\frac{\varphi+1}{2}$, la relation divisée par ε devient, pour cette valeur de z, $\varepsilon^{\varphi-1}-\varepsilon^{\frac{\varphi-1}{2}}+1\equiv 0$, et, par suite, $\varepsilon^{3.\frac{\varphi-1}{2}}+1\equiv 0$, résultat absurde, puisqu'il donne $2\equiv 0$ pour $\varphi=1$; $\varepsilon^3\equiv-1$ pour $\varphi=3$; et, pour toutes les autres valeurs de φ, $\varepsilon^{3(\varphi-1)}\equiv 1$.

Reste donc la forme $\varepsilon^1-\varepsilon^{\varphi-1}\equiv 1$, dont l'examen exige quelques développements, et qui n'est qu'un cas particulier de la forme $\varepsilon^u\pm\varepsilon^{\varphi-u}\equiv e$.

Cette relation $\varepsilon^u\pm\varepsilon^{-u}\equiv e$, dans laquelle e représente un nombre donné, a cela de remarquable que, si on élève ses deux membres à une puissance p quelconque, elle conserve sa forme primitive, le premier membre restant un binôme en ε dont le second membre exprime la valeur numérique. En effet la loi, supposée vraie jusqu'à la puissance $p-2$, se vérifie pour la puissance p; il suffit, pour cette vérification, d'élever à cette puissance p la relation $\varepsilon^u\pm\varepsilon^{-u}\equiv e$, et de grouper deux à deux les termes du développement qui ont les mêmes coefficients (*) : on trouve sans difficulté $\varepsilon^{pu}\pm\varepsilon^{-pu}\equiv E$. Remarquons toutefois qu'on ne trouvera $\varepsilon^{pu}-\varepsilon^{-pu}\equiv E$ que si p est impair, et qu'on soit parti de $\varepsilon^u-\varepsilon^{-u}\equiv e$. Le binôme de Newton servirait donc à former les diverses relations de cette forme; mais on peut obtenir des formules plus rapides.

Considérons en effet l'identité

$$(1)\quad \varepsilon^{(p+1)u}\pm\varepsilon^{-(p+1)u}=(\varepsilon^{pu}\pm\varepsilon^{-pu})(\varepsilon^u+\varepsilon^{-u})-(\varepsilon^{(p-1)u}\pm\varepsilon^{-(p-1)u}),$$

dans laquelle il faut prendre ensemble les signes supérieurs, et ensemble les signes inférieurs; nous voyons que les termes $(\varepsilon^{pu}+\varepsilon^{-pu})$, $(\varepsilon^{pu}-\varepsilon^{-pu})$ forment deux séries *récurrentes* du second ordre, dont *l'échelle de relation* est $(\varepsilon^u+\varepsilon^{-u})$ et -1. En voici deux autres dont *l'échelle de relation* est

(*) Si p est pair, le nombre des termes du développement est impair; mais le terme, qui se trouve à égale distance des extrêmes, est numérique.

$(\varepsilon^u - \varepsilon^{-u})$ et 1, et dans lesquelles le second terme du binôme change alternativement de signes :

$$(2)\quad \varepsilon^{(p+1)u} \pm \varepsilon^{-(p+1)u} = (\varepsilon^{pu} \mp \varepsilon^{-pu})(\varepsilon^u - \varepsilon^{-u}) + (\varepsilon^{(p-1)u} \pm \varepsilon^{-(p-1)u}).$$

Si on ne veut former que les puissances paires ou les puissances impaires, on aura de même les formules

$$(3)\quad \varepsilon^{(p+2)u} \pm \varepsilon^{-(p+2)u} = (\varepsilon^{pu} \pm \varepsilon^{-pu})(\varepsilon^{2u} + \varepsilon^{-2u}) - (\varepsilon^{(p-2)u} \pm \varepsilon^{-(p-2)u}),$$

$$(4)\quad \varepsilon^{(p+2)u} \pm \varepsilon^{-(p+2)u} = (\varepsilon^{pu} \mp \varepsilon^{-pu})(\varepsilon^{2u} - \varepsilon^{-2u}) + (\varepsilon^{(p-2)u} \pm \varepsilon^{-(p-2)u})$$

qui donneront les puissances paires ou les puissances impaires, suivant qu'on substituera à p la suite des nombres pairs ou celle des nombres impairs (*).

Cela posé, formons les puissances impaires de $\varepsilon^u - \varepsilon^{-u} \equiv 1$, en prenant la formule (3) avec les signes inférieurs ; *l'échelle de relation* sera 3 et -1, puisqu'en carrant $\varepsilon^u - \varepsilon^{-u} \equiv 1$, on trouve $\varepsilon^{2u} + \varepsilon^{-2u} \equiv 3$; et, comme $\varepsilon^u - \varepsilon^{-u} \equiv 1$ donne directement $\varepsilon^{3u} - \varepsilon^{-3u} \equiv 4$, nous obtiendrons pour le second membre des diverses relations $\varepsilon^{pu} - \varepsilon^{-pu} \equiv E$, les valeurs numériques

1, 4, 11, 29, 76, 199, 521, 1364, 3571, 9349, 24476,....

correspondant, terme pour terme, aux puissances de ε

u, $3u$, $5u$, $7u$, $9u$, $11u$, $13u$, $15u$, $17u$, $19u$, $21u$,....

Cette série se continuerait sans difficulté. Voici maintenant son utilité pour démontrer l'impossibilité de la relation $\varepsilon^u - \varepsilon^{-u} \equiv 1$, et par conséquent celle de $\varepsilon^1 - \varepsilon^{-1} \equiv 1$.

Observons d'abord qu'à cause de $\varepsilon^\varphi \equiv 1$, on devra avoir également $\varepsilon^{\varphi u} \equiv 1$; et, comme $\varepsilon^{-\varphi u}$ n'est autre chose que $\varepsilon^{u(\varphi - u)}$, on aura de même $\varepsilon^{-\varphi u} \equiv 1$. Ainsi le premier membre de chacune des relations $\varepsilon^{pu} - \varepsilon^{-pu} \equiv E$ devient $1 - 1$ ou zéro, lorsque le coefficient de u dans l'exposant de ε se trouve égal à φ. La série donnera donc :

pour $\varphi = 5$, $11 \equiv 0$; pour $\varphi = 7$, $29 \equiv 0$; pour $\varphi = 11$, $199 \equiv 0$;
pour $\varphi = 13$, $521 \equiv 0$; pour $\varphi = 17$, $3571 \equiv 0$; pour $\varphi = 19$, $9349 \equiv 0$.

(*) Voir la troisième note sur l'emploi des formules et leur généralisation, page 22.

Or tous ces nombres sont *premiers*, et ils donnent :

$11 = 2.5 + 1$; $29 = 2.2.7 + 1$; $199 = 2.3.3.11 + 1$; $521 = 2.2.2.5.13 + 1$; $3571 = 2.3.5.7.17 + 1$; $9349 = 2.2.3.19.41 + 1$.

On en déduit, en omettant les cas de $n = 1$ et de $n = 2$, puisque n doit être plus grand que 2, les conséquences suivantes.

Les deux premiers nombres, qui correspondent, 11 à $\varphi = 5$, et 29 à $\varphi = 7$, ne peuvent être de la forme $2k\varphi n + 1$. Les deux suivants ne pourraient être de cette forme que dans un seul cas, savoir 199 qui se rapporte à $\varphi = 11$, pour $n = 3$; et 521 qui se rapporte à $\varphi = 13$, pour $n = 5$. Le cinquième nombre, qui correspond à $\varphi = 17$, ne peut être de la forme $2k\varphi n + 1$ que si on suppose à n l'une des valeurs 3, 5, 7; et, dans chacun de ces cas, un seul facteur θ resterait excepté, savoir 3571. Enfin 9349, qui appartient à l'hypothèse de $\varphi = 19$, ne saurait être de la forme $2k\varphi n + 1$ que si n avait l'une des valeurs 3 ou 41; et, dans chacun de ces deux cas, le théorème n'en serait pas moins vrai, quel que fût θ, un seul facteur excepté, 9349.

L'observation faite à la fin du principe précédent, nous dispense d'aller plus loin dans l'examen des valeurs de φ. Le théorème peut donc être considéré comme démontré généralement, puisque, pour chaque valeur de φ, les exceptions à faire ne comprendraient jamais qu'un nombre limité de facteurs θ relatifs à certaines valeurs déterminées de n (*).

Nous ferons, en terminant, une remarque analogue à celle qui a été faite page 6, c'est qu'en formant la puissance φ de $\varepsilon^{u} - \varepsilon^{-u} \equiv 1$, ce qui conduit à $E \equiv 0$ quand φ est impair, on trouve pour $E - 1$ un multiple de φ (**).

(*) Voir la quatrième note, page 22.

(**) On peut généraliser ainsi : Le nombre E, que l'on trouve pour $(a\varepsilon^{u})^{\varphi} + (b\varepsilon^{-u})^{\varphi}$ en formant la puissance φ de $a\varepsilon^{u} + b\varepsilon^{-u} \equiv e$, satisfait à la condition $E - e = M\varphi$. En effet, le binôme donne :

$$(a\varepsilon^{u})^{\varphi} + (b\varepsilon^{-u})^{\varphi} + m\varphi \equiv e^{\varphi}; \quad \text{donc} \quad E - e = e^{\varphi} - e - m\varphi = e(e^{\varphi-1} - 1) - m\varphi:$$

or $e^{\varphi-1} - 1$ est divisible par φ, φ étant *premier*.

TROISIÈME PRINCIPE.

Impossibilité de la relation $1+\varepsilon+\varepsilon^2 \equiv 0$ pour chacune des valeurs $z=3$, $z=\varphi-2$,

$$z=\frac{m\varphi+1}{3},\quad z=\frac{m\varphi+2}{3},\quad z=\frac{\varphi-1}{2},\quad z=\frac{\varphi+3}{2}.$$

Tous ces cas se réduisent à celui de $z=3$, suivant le troisième principe du premier livre, page 7. C'est donc ce cas seulement qu'il s'agit d'examiner. Nous commencerons par exposer les principes généraux de cet examen, et nous les appliquerons ensuite aux premières valeurs de φ, à partir de $\varphi=7$, suivant ce qui a été observé à la page 13 du premier livre.

La relation $1+\varepsilon+\varepsilon^3 \equiv 0$ peut être mise sous la forme $\varepsilon+\varepsilon^{\varphi-1} \equiv -\varepsilon^{\varphi-2}$. Formons successivement les carrés de cette relation ; nous aurons la suite

$$\varepsilon^2+\varepsilon^{-1} \equiv -\varepsilon^{-2};\quad \varepsilon^4+\varepsilon^{-2} \equiv \varepsilon^{-4}-2;\quad \varepsilon^8+5\varepsilon^{-4} \equiv \varepsilon^{-8}+2;$$
$$\varepsilon^{16}+21\varepsilon^{-8} \equiv \varepsilon^{-16}-6;\quad \varepsilon^{32}+453\varepsilon^{-16} \equiv \varepsilon^{-32}-6;\quad \varepsilon^{64}+20522\varepsilon^{-32} \equiv \varepsilon^{-64}-870;\ldots$$

On peut former une autre série du même genre. En effet, le cube de $\varepsilon^2+\varepsilon^{-1} \equiv -\varepsilon^{-2}$ est $\varepsilon^3+\varepsilon^{-3} \equiv -\varepsilon^{-6}+3\varepsilon^{-2}$; et, comme $\varepsilon^2+\varepsilon^{-1}+\varepsilon^{-2} \equiv 0$ donne $3+3\varepsilon^{-2}+3\varepsilon^{-3} \equiv 0$, on obtient, en éliminant $3\varepsilon^{-2}$ du résultat précédent, $\varepsilon^3+4\varepsilon^{-3} \equiv -\varepsilon^{-6}-3$. Si on forme alors les carrés successifs de cette dernière relation, on aura la série

$$\varepsilon^3+4\varepsilon^{-3} \equiv -\varepsilon^{-6}-3;\quad \varepsilon^6+10\varepsilon^{-6} \equiv \varepsilon^{-12}+1;\quad \varepsilon^{12}+98\varepsilon^{-12} \equiv \varepsilon^{-24}-19;$$
$$\varepsilon^{24}+9642\varepsilon^{-24} \equiv \varepsilon^{-48}+165;\ldots\ (*)$$

Voici maintenant l'utilité de ces deux séries pour démontrer l'impossibilité de la relation $1+\varepsilon+\varepsilon^3 \equiv 0$. La méthode est générale : elle consiste à éliminer ε entre les relations à exposants égaux que fournissent nécessairement les séries, puisque les exposants s'y reproduisent périodiquement et dans l'une et dans l'autre. Il en résulte une condition numé-

---

(*) On peut établir de pareilles séries pour toutes les relations de la forme $a\varepsilon^{\alpha}+b\varepsilon^{-\alpha} \equiv c\varepsilon^{2\alpha}$. Voir la note cinquième, page 25.

rique qui démontre le principe, sauf l'exception possible d'un nombre limité de facteurs θ relatifs à certaines valeurs déterminées de n (*). Lorsque l'on peut trouver deux conditions numériques $A \equiv 0$, $A' \equiv 0$, la décomposition en facteurs, difficile pour les grands nombres, n'a pas besoin d'être opérée sur A ni sur A', mais bien seulement sur leur plus grand commun diviseur D, la condition $D \equiv 0$ étant la conséquence des deux premières.

Nous passons aux applications.

Premier cas, $\varphi = 7$. On trouve, dans la seconde série, $\varepsilon^6 + 10\varepsilon \equiv \varepsilon^2 + 1$; et l'on a, dans la première, $\varepsilon + \varepsilon^6 \equiv -\varepsilon^5$ ou $\varepsilon^2 + 1 \equiv -\varepsilon^6$. L'élimination de ε^2 donne $\varepsilon^6 + 5\varepsilon \equiv 0$ ou $1 + 5\varepsilon^2 \equiv 0$. Éliminant de nouveau ε^2, nous obtenons $5\varepsilon^6 \equiv -4$, et, par suite, $25\varepsilon \equiv 4$; de sorte qu'en multipliant entre eux les deux derniers résultats, on arrive à $141 \equiv 0$. Or 141, qui est égal à 3.47, ne contient aucun facteur *premier* de la forme $2k\varphi n + 1$ pour $\varphi = 7$. On pourrait encore de $5\varepsilon^2 \equiv -1$ déduire $125\varepsilon^6 \equiv -1$, qui, combiné avec $5\varepsilon^6 \equiv -4$, donne $99 \equiv 0$.

Deuxième cas, $\varphi = 11$. On trouve, dans la première série, $\varepsilon^8 + 21\varepsilon^3 \equiv \varepsilon^6 - 6$, et, dans la seconde, $\varepsilon^3 + 4\varepsilon^8 \equiv -\varepsilon^5 - 3$ ou $\varepsilon^6 + 4 \equiv -\varepsilon^8 - 3\varepsilon^3$. L'élimination de ε^8 donne $9\varepsilon^3 \equiv \varepsilon^6 - 1$ ou $\varepsilon^3 - \varepsilon^8 \equiv 9$; celle de ε^6 conduit à $\varepsilon^8 + 12\varepsilon^3 \equiv -5$: on obtiendra donc, par l'élimination successive de ε^3 et de ε^8 entre les deux derniers résultats, $13\varepsilon^8 \equiv -113$, $13\varepsilon^3 \equiv 4$, et, par conséquent, $621 \equiv 0$. Or 621, qui est égal à $3.3.3.23$, ne contient qu'un seul facteur *premier* de la forme $2k\varphi n + 1$ pour $\varphi = 11$, savoir 23, dans l'hypothèse de $n = 1$.

(*) Il n'est même pas nécessaire d'éliminer complétement ε entre les relations des séries; il suffit d'éliminer deux des trois puissances de ε, ou seulement celle du second membre. Dans le premier cas, on obtient une relation de la forme $a\varepsilon^n \equiv b$, qui donne aussitôt $a^\varphi \equiv b^\varphi$; et, dans le second, on trouve une relation de la forme $a\varepsilon^n + b\varepsilon^{-n} \equiv e$, d'où l'on déduit $a^\varphi + b^\varphi \equiv E$ en formant la puissance φ du binôme d'après les méthodes exposées. Malheureusement ces procédés, quoique très-simples, conduisent le plus souvent à des nombres considérables.

Troisième cas, $\varphi = 13$. Combinons $\varepsilon^{12} + 98\varepsilon \equiv \varepsilon^2 - 19$ de la seconde série avec $\varepsilon + \varepsilon^{12} \equiv -\varepsilon^{11}$ ou $\varepsilon^2 + 1 \equiv -\varepsilon^{12}$ de la première. Si on élimine ε^2, on trouve $\varepsilon^{12} + 49\varepsilon \equiv -10$; et, si on élimine ε^{12}, on obtient $49\varepsilon \equiv \varepsilon^2 - 9$ ou $49 \equiv \varepsilon - 9\varepsilon^{12}$. Ces deux résultats conduisent, par l'élimination successive de ε^{12} et de ε, aux relations $442\varepsilon \equiv -41$, $442\varepsilon^{12} \equiv -2411$ lesquelles, multipliées entre elles, donnent $96513 \equiv 0$. Or 96513, qui est égal à $3.53.607$, ne contient aucun facteur *premier* de la forme $2k\varphi n + 1$ pour $\varphi = 13$, si ce n'est 53, dans le cas de $n = 1$ et dans celui de $n = 2$. En effet $53 = 2.2.13 + 1$, et $607 = 2.3.101 + 1$.

Quatrième cas, $\varphi = 17$. On trouve, dans la première série, $\varepsilon^{16} + 453\varepsilon \equiv \varepsilon^2 - 6$, et $\varepsilon + \varepsilon^{16} \equiv -\varepsilon^{15}$ ou $\varepsilon^2 + 1 \equiv -\varepsilon^{16}$. Si on élimine ε^2, on obtient $2\varepsilon^{16} + 453\varepsilon \equiv -7$; et, si on élimine ε^{16}, on a $453\varepsilon \equiv 2\varepsilon^2 - 5$ ou $453 \equiv 2\varepsilon - 5\varepsilon^{16}$. Il reste à éliminer ε^{16}, puis ε, ce qui donne $2269\varepsilon \equiv 871$, $2269\varepsilon^{16} \equiv -205223$. En conséquence on trouve, après avoir multiplié membre à membre et réduit, $1838975 94 \equiv 0$. Mais ce dernier nombre, qui est égal à $2.3.3.3.239.14249$, n'admet d'autre facteur *premier* de la forme $2k\varphi n + 1$, pour $\varphi = 17$, que 239 dont la valeur est $2.7.17 + 1$, attendu que $14249 = 2.2.2.13.137 + 1$. Ainsi, dans les cas particuliers de $n = 1$ et de $n = 7$, un seul facteur θ échapperait à l'analyse (*).

Cinquième cas, $\varphi = 19$. La première série donne $\varepsilon^{16} + 453\varepsilon^3 \equiv \varepsilon^6 - 6$, et la seconde $\varepsilon^3 + 4\varepsilon^{16} \equiv -\varepsilon^{13} - 3$ ou $\varepsilon^6 + 4 \equiv -\varepsilon^{16} - 3\varepsilon^3$. Éliminant ε^6, nous obtenons $\varepsilon^{16} + 228\varepsilon^3 \equiv -5$; puis l'élimination de ε^{16} fait trouver $225\varepsilon^3 \equiv \varepsilon^6 - 1$ ou $225 \equiv \varepsilon^3 - \varepsilon^{16}$. Faisant alors disparaître successivement ε^{16} et ε^3 entre les deux dernières relations, on trouve $229\varepsilon^3 \equiv 220$, $229\varepsilon^{16} \equiv -51305$, de sorte qu'en multipliant ces résultats entre eux membre à membre, on arrive à $11339541 \equiv 0$. Or ce nombre, qui est égal à $3.3.3.457.919$, ne saurait avoir de diviseur *premier* de la forme $2k\varphi n + 1$ que si on suppose $n = 1$, $n = 2$, ou $n = 3$; encore, dans cha-

(*) Voir la note sixième, page 26.

cun de ces cas, le seul facteur 457 resterait excepté. On a, en effet, $919 = 2.3.3.3.17 + 1$, et $457 = 2.2.2.3.19 + 1$.

QUATRIÈME PRINCIPE.

Impossibilité de la relation $1 + \varepsilon \equiv \varepsilon^z$ pour $z = 3$, $z = \varphi - 2$, $z = \frac{m\varphi + 1}{3}$, $z = \frac{m\varphi + 2}{3}$, $z = \frac{\varphi - 1}{2}$, $z = \frac{\varphi + 3}{2}$.

D'après le quatrième principe du premier livre, pages 9 et 13, tous ces cas se réduisent à un seul, celui de $z = 3$, valeur qu'il faut essayer dans les trois relations

$$1 + \varepsilon - \varepsilon^z \equiv 0, \quad 1 - \varepsilon + \varepsilon^z \equiv 0, \quad -1 + \varepsilon + \varepsilon^z \equiv 0.$$

En y faisant $z = 3$, et en divisant par ε^2, on met ces relations sous la forme

$$-\varepsilon + \varepsilon^{-1} \equiv -\varepsilon^{-2}, \quad \varepsilon - \varepsilon^{-1} \equiv -\varepsilon^{-2}, \quad \varepsilon + \varepsilon^{-1} \equiv \varepsilon^{-2}.$$

Chacune d'elles donnera lieu à deux séries que l'on formera comme les précédentes. La méthode étant la même, nous passons immédiatement à l'application pour les premières valeurs de φ, à partir de $\varphi = 7$, eu égard à l'observation faite au principe troisième du premier livre, page 13, et déjà rappelée au commencement du principe précédent.

Premièrement. Impossibilité de la relation $-\varepsilon^1 + \varepsilon^{-1} \equiv -\varepsilon^{-2}$ pour $\varphi = 7$, $\varphi = 11$, $\varphi = 13$, $\varphi = 17$, $\varphi = 19$.

Les deux séries auxquelles conduit $-\varepsilon^1 + \varepsilon^{-1} \equiv -\varepsilon^{-2}$ sont :

$$\begin{array}{ll}
\varepsilon^2 + \varepsilon^{-2} \equiv \varepsilon^{-4} + 2, & \varepsilon^3 + 2\varepsilon^{-3} \equiv \varepsilon^{-6} + 3, \ (*) \\
\varepsilon^4 - 3\varepsilon^{-4} \equiv \varepsilon^{-8} + 2, & \varepsilon^6 - 2\varepsilon^{-6} \equiv \varepsilon^{-12} + 5, \\
\varepsilon^8 + 5\varepsilon^{-8} \equiv \varepsilon^{-16} + 10, & \varepsilon^{12} - 6\varepsilon^{-12} \equiv \varepsilon^{-24} + 29, \\
\varepsilon^{16} + 5\varepsilon^{-16} \equiv \varepsilon^{-32} + 90, & \varepsilon^{24} - 22\varepsilon^{-24} \equiv \varepsilon^{-48} + 853, \\
\dots\dots\dots\dots & \dots\dots\dots\dots
\end{array}$$

(*) On a vu précédemment, page 10, comment la relation $\varepsilon^3 + 4\varepsilon^{-3} \equiv -\varepsilon^{-6} - 3$ a été déduite de $\varepsilon^1 + \varepsilon^{-1} \equiv -\varepsilon^{-2}$. Le procédé est général.

Premier cas, $\varphi = 7$. On trouve, dans la première serie, $\varepsilon + 5\varepsilon^6 \equiv \varepsilon^5 + 10$, et on a $\varepsilon - \varepsilon^6 \equiv \varepsilon^5$. Ces relations donnent immédiatement $3\varepsilon^6 \equiv 5$ ou $3\varepsilon^5 \equiv 5\varepsilon^6$. Éliminant de nouveau ε^5, on a $3\varepsilon \equiv 8\varepsilon^6$, et, par suite, $9\varepsilon \equiv 40$: on en conclut $173 \equiv 0$. Or 173, qui est *premier*, est égal à $2.2.43 + 1$, et ne saurait être de la forme $2k\varphi n + 1$ pour $\varphi = 7$.

Deuxième cas, $\varphi = 11$. Si on combine $\varepsilon^8 + 5\varepsilon^3 \equiv \varepsilon^6 + 10$ de la première série avec $\varepsilon^3 + 2\varepsilon^8 \equiv \varepsilon^5 + 3$ ou $\varepsilon^6 + 2 \equiv \varepsilon^8 + 3\varepsilon^3$ de la seconde, on trouve aussitôt $\varepsilon^3 \equiv 4$ ou $\varepsilon^6 \equiv 4\varepsilon^3$. Éliminant alors ε^6, nous obtenons $2 + \varepsilon^3 \equiv \varepsilon^8$, et, par conséquent, $\varepsilon^8 \equiv 6$: on arrive donc à $23 \equiv 0$. Or 23, qui est égal à $2.11 + 1$, ne saurait être de la forme $2k\varphi n + 1$ pour $\varphi = 11$, si ce n'est dans le cas de $n = 1$.

Troisième cas, $\varphi = 13$. On voit, dans la seconde série, $\varepsilon^{12} - 6\varepsilon \equiv \varepsilon^2 + 29$, et l'on a $\varepsilon - \varepsilon^{12} \equiv \varepsilon^{11}$ ou $\varepsilon^2 - 1 \equiv \varepsilon^{12}$. On en déduit facilement $\varepsilon \equiv -5$ ou $\varepsilon^2 \equiv -5\varepsilon$. Éliminant de nouveau ε^2, nous obtenons $\varepsilon^{12} \equiv 24$, et, par conséquent, $121 \equiv 0$. Mais 121, qui est égal à 11.11, n'a aucun diviseur *premier* de la forme $2k\varphi n + 1$ pour $\varphi = 13$.

Quatrième cas, $\varphi = 17$. La première série donne $\varepsilon^{16} + 5\varepsilon \equiv \varepsilon^2 + 90$, et l'on a $\varepsilon - \varepsilon^{16} \equiv \varepsilon^{15}$ ou $\varepsilon^2 - 1 \equiv \varepsilon^{16}$. On obtient, sans difficulté, $5\varepsilon \equiv 91$ ou $5\varepsilon^2 \equiv 91\varepsilon$. Il en résulte $91\varepsilon \equiv 5\varepsilon^{16} + 5$, puis $25\varepsilon^{16} \equiv 8256$, et enfin $751171 \equiv 0$. Mais ce dernier nombre, qui est égal à 137.5483, ne contient aucun facteur *premier* de la forme $2k\varphi n + 1$ dans le cas de $\varphi = 17$, à l'exception de 137 pour $n = 1$ ou $n = 2$, puisque $137 = 2.2.2.17 + 1$, et que 5483, qui est *premier*, est égal à $2.2741 + 1$.

Cinquième cas, $\varphi = 19$. On a $\varepsilon^{16} + 5\varepsilon^3 \equiv \varepsilon^6 + 90$, et $\varepsilon^3 + 2\varepsilon^{16} \equiv \varepsilon^{13} + 3$ ou $\varepsilon^6 + 2 \equiv \varepsilon^{16} + 3\varepsilon^3$: donc $\varepsilon^3 \equiv 44$ ou $\varepsilon^6 \equiv 44\varepsilon^3$, et, par suite, $\varepsilon^{16} \equiv 41\varepsilon^3 + 2$, $\varepsilon^{16} \equiv 1806$. En conséquence on trouvera $79463 \equiv 0$. Mais 79463, qui est égal à 229.347, ne saurait être divisible par aucun facteur *premier* de la forme $2k\varphi n + 1$ pour $\varphi = 19$, que si on suppose $n = 1$, $n = 2$ ou $n = 3$; et, pour chacun de ces cas, il n'y aurait que le facteur 229 qui ferait exception au principe : on a, en effet, $229 = 2.2.3.19 + 1$, et $347 = 2.173 + 1$.

Secondement. Impossibilité de la deuxième relation $\varepsilon^{1}-\varepsilon^{-1}\equiv-\varepsilon^{-2}$ pour $\varphi=7$, $\varphi=11$, $\varphi=13$, $\varphi=17$, $\varphi=19$.

Les séries auxquelles conduit $\varepsilon^{1}-\varepsilon^{-1}\equiv-\varepsilon^{-2}$, sont :

$$\begin{array}{ll}
\varepsilon^{2}+\varepsilon^{-2}\equiv\varepsilon^{-4}+2, & \varepsilon^{3}+2\varepsilon^{-3}\equiv-\varepsilon^{-6}-3,\\
\varepsilon^{4}-3\varepsilon^{-4}\equiv\varepsilon^{-8}+2, & \varepsilon^{6}-2\varepsilon^{-6}\equiv\varepsilon^{-12}+5,\\
\varepsilon^{8}+5\varepsilon^{-8}\equiv\varepsilon^{-16}+10, & \varepsilon^{12}-6\varepsilon^{-12}\equiv\varepsilon^{-24}+29,\\
\varepsilon^{16}+5\varepsilon^{-16}\equiv\varepsilon^{-32}+90, & \varepsilon^{24}-22\varepsilon^{-24}\equiv\varepsilon^{-48}+853,\\
\dots\dots\dots\dots & \dots\dots\dots\dots
\end{array}$$

Premier cas, $\varphi=7$. Combinons $\varepsilon^{6}-2\varepsilon\equiv\varepsilon^{2}+5$ de la seconde série avec $\varepsilon-\varepsilon^{6}\equiv-\varepsilon^{5}$ ou $\varepsilon^{2}-1\equiv-\varepsilon^{6}$. L'élimination de ε^{2} donne $\varepsilon^{6}-\varepsilon\equiv3$ ou $1-\varepsilon^{2}\equiv3\varepsilon$; éliminant de nouveau ε^{2}, on trouve $3\varepsilon\equiv\varepsilon^{6}$: donc $2\varepsilon\equiv3$, $2\varepsilon^{6}\equiv9$, et, par suite, $23\equiv0$, condition absurde pour $\varphi=7$, puisque $23=2.11+1$.

Deuxième cas, $\varphi=11$. On trouve, dans les séries, $\varepsilon^{8}+5\varepsilon^{8}\equiv\varepsilon^{6}+10$, puis $\varepsilon^{3}+2\varepsilon^{8}\equiv-\varepsilon^{5}-3$ ou $\varepsilon^{6}+2\equiv-\varepsilon^{8}-3\varepsilon^{3}$; on en déduit $\varepsilon^{8}+4\varepsilon^{3}\equiv4$ ou $1+4\varepsilon^{6}\equiv4\varepsilon^{3}$. Éliminant ε^{6}, puis ε^{8}, on trouve $23\equiv0$, résultat impossible pour $\varphi=11$, si ce n'est dans l'hypothèse de $n=1$.

Troisième cas, $\varphi=13$. Il suffit de combiner $\varepsilon^{12}-6\varepsilon\equiv\varepsilon^{2}+29$ avec $\varepsilon-\varepsilon^{12}\equiv-\varepsilon^{11}$ qui est la même chose que $\varepsilon^{2}-1\equiv-\varepsilon^{12}$. On trouve, en effet, par l'élimination de ε^{2}, $\varepsilon^{12}-3\varepsilon\equiv15$ ou $1-3\varepsilon^{3}\equiv15\varepsilon$. Éliminant de nouveau ε^{2}, on obtient $3\varepsilon^{12}-2\equiv15\varepsilon$; et, faisant disparaître alors successivement ε^{12} et ε, on arrive à $6\varepsilon\equiv43$ et à $2\varepsilon^{12}\equiv73$, d'où l'on conclut définitivement $3127\equiv0$. Or 3127, qui est égal à 53.59, n'a d'autre diviseur θ, pour $\varphi=13$, que 53 dans le cas de $n=1$, ou dans celui de $n=2$, puisque $53=2.2.13+1$, et que $59=2.29+1$.

Quatrième cas, $\varphi=17$. De $\varepsilon^{16}+5\varepsilon\equiv\varepsilon^{2}+90$ avec $\varepsilon-\varepsilon^{16}\equiv-\varepsilon^{15}$ ou $\varepsilon^{2}-1\equiv-\varepsilon^{16}$, on déduit $2\varepsilon^{16}+5\varepsilon\equiv91$ ou $2+5\varepsilon^{2}\equiv91\varepsilon$. On trouve ensuite $7-5\varepsilon^{16}\equiv91\varepsilon$, puis $157\varepsilon\equiv-441$ et $157\varepsilon^{16}\equiv8246$, d'où l'on déduit enfin $3661135\equiv0$. Or $3661135=5.103.7109$: ce nombre ne contient donc qu'un seul facteur *premier* de la forme $2k\varphi n+1$ pour $\varphi=17$, savoir 103, dans les cas de $n=1$ et de $n=3$, puisque $7109=2.2.1777+1$ et que $103=2.3.17+1$.

Cinquième cas, $\varphi = 19$. Combinons $\varepsilon^{16} + 5\varepsilon^3 \equiv \varepsilon^6 + 90$ avec $\varepsilon^3 + 2\varepsilon^{16} \equiv -\varepsilon^{13} - 3$ ou $\varepsilon^6 + 2 \equiv -\varepsilon^{16} - 3\varepsilon^3$; nous trouvons, en éliminant ε^6, $\varepsilon^{16} + 4\varepsilon^3 \equiv 44$; et, si l'on fait disparaître ε^{16}, on obtient $\varepsilon^3 \equiv \varepsilon^6 + 46$ ou $1 \equiv \varepsilon^3 + 46\varepsilon^{16}$: donc $183\varepsilon^{16} \equiv -40$, et, par suite, $183\varepsilon^3 \equiv 2023$. En conséquence on arrivera à $114409 \equiv 0$. Mais 114409, qui est égal à 191.599, ne contient, pour $\varphi = 19$, qu'un seul facteur θ, savoir 191, dans les cas de $n = 1$ et de $n = 5$. On a, en effet, $191 = 2.5.19 + 1$, et $599 = 2.13.23 + 1$.

Troisièmement. Impossibilité de la relation $\varepsilon^1 + \varepsilon^{-1} \equiv \varepsilon^{-2}$ pour $\varphi = 7$, $\varphi = 11$, $\varphi = 13$, $\varphi = 17$, $\varphi = 19$.

Les séries, auxquelles conduit la relation $\varepsilon^1 + \varepsilon^{-1} \equiv \varepsilon^{-2}$, sont :

$$\begin{array}{ll}
\varepsilon^2 + \varepsilon^{-2} \equiv \varepsilon^{-4} - 2, & \varepsilon^3 + 4\varepsilon^{-3} \equiv \varepsilon^{-6} + 3, \\
\varepsilon^4 + 5\varepsilon^{-4} \equiv \varepsilon^{-8} + 2, & \varepsilon^6 + 10\varepsilon^{-6} \equiv \varepsilon^{-12} + 1, \\
\varepsilon^8 + 21\varepsilon^{-8} \equiv \varepsilon^{-16} - 6, & \varepsilon^{12} + 98\varepsilon^{-12} \equiv \varepsilon^{-24} - 19. \\
\varepsilon^{16} + 453\varepsilon^{-16} \equiv \varepsilon^{-32} - 6, & \ldots\ldots\ldots\ldots\ldots\ldots \\
\ldots\ldots\ldots\ldots\ldots\ldots & \ldots\ldots\ldots\ldots\ldots\ldots
\end{array}$$

Premier cas, $\varphi = 7$. La relation $\varepsilon^4 + 5\varepsilon^3 \equiv \varepsilon^6 + 2$, combinée avec $\varepsilon^3 + 4\varepsilon^4 \equiv \varepsilon + 3$ ou $\varepsilon^6 + 4 \equiv \varepsilon^4 + 3\varepsilon^3$, donne $\varepsilon^3 \equiv -1$, et conduit, par conséquent, à $2 \equiv 0$.

Deuxième cas, $\varphi = 11$. On a $\varepsilon^8 + 21\varepsilon^3 \equiv \varepsilon^6 - 6$, $\varepsilon^3 + 4\varepsilon^8 \equiv \varepsilon^5 + 3$ ou $\varepsilon^6 + 4 \equiv \varepsilon^8 + 3\varepsilon^3$: on aura donc $9\varepsilon^3 \equiv -5$ ou $9\varepsilon^6 \equiv -5\varepsilon^3$. On en déduira, par l'élimination de ε^6 et de ε^3, $81\varepsilon^8 \equiv 484$; et, par suite, $3149 \equiv 0$. Mais $3149 = 47.67$: donc ce nombre ne serait divisible que par un seul facteur θ, dans le cas de $\varphi = 11$, savoir 67, pour $n = 1$ et pour $n = 3$, puisque $67 = 2.3.11 + 1$ et que $47 = 2.23 + 1$.

Troisième cas, $\varphi = 13$. Combinez $\varepsilon^{12} + 98\varepsilon \equiv \varepsilon^2 - 19$ avec $\varepsilon + \varepsilon^{12} \equiv \varepsilon^{11}$ ou $\varepsilon^2 + 1 \equiv \varepsilon^{12}$; vous obtenez $49\varepsilon \equiv -10$ ou $49\varepsilon^2 \equiv -10\varepsilon$. L'élimination de ε^2 donnera $2401\varepsilon^{12} \equiv 2501$. En conséquence on arrivera à la condition $142659 \equiv 0$. Mais 142659, qui est égal à $3.3.11.11.131$, n'a d'autre diviseur θ, pour $\varphi = 13$, que 131, dans le cas de $n = 1$ et dans celui de $n = 5$, puisque $131 = 2.5.13 + 1$.

Quatrième cas, $\varphi = 17$. En comparant $\varepsilon^{16} + 453\varepsilon \equiv \varepsilon^2 - 6$ avec $\varepsilon + \varepsilon^{16} \equiv \varepsilon^{15}$ ou $\varepsilon^2 + 1 \equiv \varepsilon^{16}$, on trouve $453\varepsilon \equiv -7$ ou $453\varepsilon^2 \equiv -7\varepsilon$, puis $453\varepsilon^{16} \equiv -7\varepsilon + 453$. On en conclura donc $205209\varepsilon^{16} \equiv 205258$, et, par suite, $94396483 \equiv 0$. Or ce dernier nombre, qui est égal à 613.153991, ne contient qu'un seul facteur θ pour $\varphi = 17$, savoir 613, dans les cas de $n = 1$, $n = 2$, $n = 3$. En effet, $613 = 2.2.3.3.17 + 1$ et $153991 = 2.3.3.5.29.59 + 1$ (*).

Cinquième cas, $\varphi = 19$. On trouve $\varepsilon^{16} + 453\varepsilon^3 \equiv \varepsilon^6 - 6$, $\varepsilon^3 + 4\varepsilon^{16} \equiv \varepsilon^{13} + 3$ ou $\varepsilon^6 + 4 \equiv \varepsilon^{16} + 3\varepsilon^3$. On en déduit $45\varepsilon^3 \equiv -1$ ou $45\varepsilon^6 \equiv -\varepsilon^3$, puis $136\varepsilon^3 + 45\varepsilon^{16} \equiv 180$, et, par suite, $2025\varepsilon^{16} \equiv 8236$ d'où $99361 \equiv 0$. Mais 99361, qui est égal à 67.1483, n'a pour $\varphi = 19$ qu'un seul diviseur *premier* de la forme $2k\varphi n + 1$, savoir 1483, puisque $67 = 2.3.11 + 1$. Cette exception n'aurait lieu que dans les hypothèses particulières $n = 1$, $n = 3$, $n = 13$, attendu que ce nombre 1483 est égal à $2.3.13.19 + 1$.

OBSERVATIONS SUR LE SECOND LIVRE.

Les principes contenus dans ce second livre résultent de méthodes générales dont l'application est toujours possible, et les facteurs θ, qu'elles n'atteignent pas, sont en nombre limité pour chaque valeur de φ. Ces facteurs ne concernent d'ailleurs que certaines valeurs particulières de n. Les théorèmes se trouvent donc démontrés généralement, ainsi que la possibilité de réduire les formes $\varepsilon^x + \varepsilon^y + \varepsilon^z \equiv 0$, $\varepsilon^x + \varepsilon^y \equiv \varepsilon^z$ aux formes $1 + \varepsilon + \varepsilon^2 \equiv 0$, $1 + \varepsilon \equiv \varepsilon^2$. Nous donnons ci-contre, pour les valeurs de φ jusqu'à 19 inclusivement, et pour n plus grand que 3, le tableau des facteurs θ qui échappent à notre analyse.

Nous avons laissé au lecteur le soin de vérifier les nombres *premiers* que nous avons déclarés tels dans l'exposition des trois derniers prin-

(*) Voir la note septième, page 26.

cipes. Mais, comme, à l'exception de 14249 et de 153991, tous ces nombres (*) sont inférieurs à 10000, on pourra consulter la table que nous venons de publier, où l'on trouve les nombres *premiers* de 1 à 10000, avec des procédés de vérification simples et rapides. Quant aux deux nombres 14249 et 153991, qui excèdent les limites de cette table, les deux dernières notes de ce mémoire dispensent, au besoin, de la considération de ces nombres.

TABLEAU

des facteurs θ qui, pour n plus grand que 3, et jusqu'à $\varphi = 19$ inclusivement, échappent aux démonstrations données pour les principes du second livre.

n	φ	θ	k	PRINCIPES.	n	φ	θ	k	PRINCIPES.
5	13	131	1	4	7	17	3571	15	2
5	13	521	4	2	7	19	174763	657	1
5	13	2731	21	1	7	19	524287	1971	1
5	13	8191	63	1	13	19	1483	3	4
5	17	3571	21	2	31	11	683	1	1
5	17	43691	257	1	41	19	9349	6	2
5	17	131071	771	1	73	19	174763	63	1
5	19	191	1	4	73	19	524287	189	1
7	13	2731	15	1	257	17	43691	5	1
7	13	8191	45	1	257	17	131071	15	1
7	17	239	1	3					

(*) Ces nombres sont peu nombreux; nous les résumons plus loin, note huitième, page 27,

NOTES DU QUATRIÈME MÉMOIRE.

Première note (*). L'impossibilité de $2^{\varphi} \equiv \pm 1$, relativement à θ, est subordonnée à cette condition unique que le résidu de $2^{2\varphi}$ soit différent de 1, ce qui, du reste, arrivera toujours pour les facteurs θ plus grands que $2^{\varphi}+1$. Voici, pour le cas où θ n'atteint pas cette limite, une règle fort simple qui réussit à déterminer une classe indéfinie de valeurs relativement auxquelles la condition $2^{2\varphi} \equiv 1$ est impossible.

Nous avons rappelé, dans notre troisième mémoire, le théorème qui sert à faire connaître, relativement à θ, le résidu de $2^{\frac{\theta-1}{2}}$. Ce résidu de $2^{k\varphi n}$, puisque $\theta = 2k\varphi n + 1$, est 1 si θ est de la forme $8p \pm 1$, et -1 si θ est de la forme $8p \pm 3$. Si donc θ est de cette dernière forme, et que k soit pair, il est clair que, -1 étant le résidu de $2^{k\varphi n}$, on ne saurait avoir ni $2^{\varphi} \equiv 1$ ni $2^{\varphi} \equiv -1$. Or, si on pose $2k\varphi n + 1 = 8p - 3$, d'où $k\varphi n = 4p - 2$, on reconnaît que k est nécessairement double d'un impair. En conséquence, toutes les fois que θ sera, pour des valeurs déterminées de φ et de n, de la forme $4k'\varphi n + 1$, avec la condition de k' impair, on sera certain de l'impossibilité de $2^{2\varphi} \equiv 1$, relativement à θ.

Ainsi, pour $\theta = 4093$ dans le cas de $\varphi = 31$ et de $n = 11$, la condition $2^{2\varphi} \equiv 1$ est absurde. Elle le serait de même pour $\theta = 7541$, dans le cas de $\varphi = 29$ et de $n = 13$, etc.... En effet, $4093 = 2.2.3.11.31 + 1$, $7541 = 2.2.5.13.29 + 1$,..., et ces nombres sont de la forme $8p - 3$.

Deuxième note (**). On peut généraliser comme il suit : Si a et b sont

(*) Voir à la page 5.

(**) Voir à la page 6.

premiers entre eux, $\frac{a^n+b^n}{a+b}-1$ et $\frac{a^n-b^n}{a-b}-1$ sont divisibles par n, pourvu que n soit un nombre *premier* qui ne divise ni $a+b$ ni $a-b$. Les nombres compris dans ces formules ne pourront avoir d'autres diviseurs communs que ceux de $2a(a^{n-1}-1)$ et de $2b(b^{n-1}-1)$, formes qui aideront à faire découvrir ces diviseurs. Ce principe général résulte de la double égalité

$$\frac{a^n+b^n}{a+b}-1=\frac{(a^{n-1}-1)a+(b^{n-1}-1)b}{a+b},$$

$$\frac{a^n-b^n}{a-b}-1=\frac{(a^{n-1}-1)a-(b^{n-1}-1)b}{a-b}.$$

En effet, en multipliant le premier de ces deux nombres par $a+b$ et le second par $a-b$, on ne supprime aucun de leurs facteurs communs. Or les facteurs communs aux deux nombres $(a^{n-1}-1)a+(b^{n-1}-1)b$, $(a^{n-1}-1)a-(b^{n-1}-1)b$, que nous désignerons par A+B et A—B, le sont à 2A et à 2B, et réciproquement ceux communs à A et à B le sont à A+B et à A—B, de sorte que, si D est le plus grand commun diviseur des nombres A et B, D ou 2D sera celui de A+B et de A—B (*), et contiendra par conséquent tous les facteurs communs aux deux nombres proposés $\frac{a^n+b^n}{a+b}-1$, $\frac{a^n-b^n}{a-b}-1$, plus les facteurs communs provenant de la multiplication du premier par $a+b$ et du second par $a-b$.

Pour aller plus loin sur cette question délicate, nous dirons que les facteurs communs, introduits par la multiplication, ne peuvent se trouver que parmi ceux de $a^{n-1}-1$ et de $b^{n-1}-1$ (**). En effet les nombres a et b, que nous supposons *premiers* entre eux, sont par cela même *premiers* avec $a+b$ et $a-b$; de sorte que, si on les supprime dans les expressions $(a^{n-1}-1)a$ et $(b^{n-1}-1)b$, cette suppression n'entraîne

(*) Ce sera 2D toutes les fois que A et B seront multiples de nombres impairs par une même puissance de 2.

(**) Ces facteurs communs aux deux binômes $a^{n-1}-1$, $b^{n-1}-1$ sont compris dans $(ab)^{n-1}-1$, comme le démontre l'identité

$$(ab)^{n-1}-1=(a^{n-1}-1)\,b^{n-1}+b^{n-1}-1.$$

avec elle la disparition d'aucun facteur introduit. Cela posé, les facteurs communs à $a+b$ et à $b^{n-1}-1$ ou $ab^{n-1}-a$, divisent $ab^{n-2}+1$, puis $a^2b^{n-3}-1,\ldots$, et $(ab)^{\frac{n-1}{2}}-1$ ou $(ab)^{\frac{n-1}{2}}+1$, suivant que $\frac{n-1}{2}$ est pair ou impair. La conclusion est la même pour les facteurs communs à $a+b$ et à $a^{n-1}-1$. On trouverait également que les facteurs communs à $a-b$ et à $b^{n-1}-1$ ou à $a^{n-1}-1$, divisent $(ab)^{\frac{n-1}{2}}-1$. Le principe inverse étant facile à établir, on pourra, pour obtenir les facteurs communs qui proviennent de la multiplication par $a+b$ et par $a-b$, chercher ceux qui divisent $a+b$ et $(ab)^{\frac{n-1}{2}}-1$ ou $(ab)^{\frac{n-1}{2}}+1$, suivant que $\frac{n-1}{2}$ est pair ou impair, et ceux qui divisent $a-b$ et $(ab)^{\frac{n-1}{2}}-1$ (*), Soit D′ le plus grand commun diviseur introduit; $\frac{D}{D'}$ ou $\frac{2D}{D'}$ sera celui des nombres proposés.

Considérons le cas particulier de $b=1$. La valeur de D sera $(a^{n-1}-1)a$; celle de D′ sera a^2-1 si a est pair, et $\frac{a^2-1}{2}$ si a est impair : donc les facteurs communs aux deux nombres $\frac{a^n+1}{a+1}-1$, $\frac{a^n-1}{a-1}-1$ seront ceux de $\frac{(a^{n-1}-1)a}{a^2-1}$ ou de $\frac{2(a^{n-1}-1)a}{a^2-1}$. C'est, du reste, ce qu'il est facile de vérifier, car les nombres proposés peuvent être mis sous la forme $\frac{(a^{n-1}-1)a}{a+1}$, $\frac{(a^{n-1}-1)a}{a-1}$, et il est clair que leur plus grand commun diviseur est $\frac{(a^{n-1}-1)a}{a^2-1}$ ou $\frac{2(a^{n-1}-1)a}{a^2-1}$, suivant que a est pair ou impair.

(*) Les deux principes direct et inverse résultent d'ailleurs des deux formes que l'on peut donner aux binômes $(ab)^{\frac{n-1}{2}}+1$ et $(ab)^{\frac{n-1}{2}}-1$, savoir :

$$\left(a^{\frac{n-1}{2}}+b^{\frac{n-1}{2}}\right)a^{\frac{n-1}{2}}-\left(a^{n-1}-1\right),\quad \left(a^{\frac{n-1}{2}}+b^{\frac{n-1}{2}}\right)b^{\frac{n-1}{2}}-\left(b^{n-1}-1\right);$$
$$-\left(a^{\frac{n-1}{2}}-b^{\frac{n-1}{2}}\right)a^{\frac{n-1}{2}}+\left(a^{n-1}-1\right),\quad \left(a^{\frac{n-1}{2}}-b^{\frac{n-1}{2}}\right)b^{\frac{n-1}{2}}+\left(b^{n-1}-1\right).$$

Troisième note (*). Pour former les diverses séries dont nous avons donné les expressions, il est nécessaire d'en connaître non-seulement l'*échelle de relation*, mais encore les deux premiers termes: On apercevra sans difficulté, dans chaque cas, les éléments dont on aura besoin. Les séries, que nous allons indiquer, n'exigent, pour se former, que l'un des éléments $\varepsilon^{u}+\varepsilon^{-u}$, $\varepsilon^{u}-\varepsilon^{-u}$, $\varepsilon^{2u}-\varepsilon^{-2u}$.

Avec la valeur numérique de $\varepsilon^{u}+\varepsilon^{-u}$, on pourra développer la première des séries (1) en la faisant commencer à $p=1$, et la première des séries (3) en la faisant commencer à $p=2$ ou à $p=3$. En effet, pour ces deux dernières hypothèses, $\varepsilon^{u}+\varepsilon^{-u}$ conduit directement à $\varepsilon^{2u}+\varepsilon^{-2u}$ et à $\varepsilon^{3u}+\varepsilon^{-3u}$.

La valeur numérique de $\varepsilon^{u}-\varepsilon^{-u}$ suffira pour former la première des séries (2) que l'on fera commencer à $p=1$; et la deuxième des séries (3) que l'on fera commencer à $p=3$. En effet, pour cette dernière série, $\varepsilon^{u}-\varepsilon^{-u}$ donne immédiatement $\varepsilon^{2u}+\varepsilon^{-2u}$ et $\varepsilon^{3u}-\varepsilon^{-3u}$.

Enfin, avec $\varepsilon^{2u}-\varepsilon^{-2u}$, on développera la première des séries (4) que l'on fera commencer à $p=2$.

Nous avons fait observer que, dans les séries (2) et (4), le second terme du binôme change de signe alternativement. On devra donc, dans la formation de chacune de ces quatre séries, prendre alternativement les deux suites de signes, en partant des signes supérieurs pour la première des séries (2) et la première des séries (4), et en partant des signes inférieurs pour la deuxième des séries (2) et la deuxième des séries (4).

Tout ce que nous avons dit, sur ce sujet, est applicable au cas où le binôme aurait des coefficients numériques a et b. On a, en effet, les mêmes identités, puisque généralement l'expression $a^{p+m}\varepsilon^{(p+m)u}\pm b^{p+m}\varepsilon^{-(p+m)u}$ est *identiquement* égale à chacune des deux expressions

$$(a^{p}\varepsilon^{pu}\pm b^{p}\varepsilon^{-pu})(a^{m}\varepsilon^{mu}+b^{m}\varepsilon^{-mu})-a^{m}b^{m}(a^{p-m}\varepsilon^{(p-m)u}\pm b^{p-m}\varepsilon^{-(p-m)u}),$$
$$(a^{p}\varepsilon^{pu}\mp b^{p}\varepsilon^{-pu})(a^{m}\varepsilon^{mu}-b^{m}\varepsilon^{-mu})+a^{m}b^{m}(a^{p-m}\varepsilon^{(p-m)u}\pm b^{p-m}\varepsilon^{-(p-m)u}),$$

Quatrième note (**). Il existe d'autres méthodes qui conduisent aux

(*) Voir à la page 8.
(**) Voir à la page 9.

mêmes résultats, et dont nous regretterions de ne pas conserver la trace.

1. Formons, avec la première des deux formules (3) de la page 8, les puissances paires de $\varepsilon^1 - \varepsilon^{-1} \equiv 1$; nous trouvons respectivement :

pour les puissances.... 2, 4, 6, 8, 10, 12, 14, 16, 18, 20...,
les résultats numériques 3, 7, 18, 47, 123, 322, 843, 2207, 5778, 15127...,

qui sont les valeurs du second membre.

Si maintenant on compare ces valeurs avec celles des puissances impaires de $\varepsilon^1 - \varepsilon^{-1} \equiv 1$ données à la page 8, on trouvera respectivement,

pour $\varphi = 5$, $\varphi = 7$, $\varphi = 11$, $\varphi = 13$, $\varphi = 17$, $\varphi = 19$,...

les résultats déjà obtenus

$11 \equiv 0$, $29 \equiv 0$, $199 \equiv 0$, $521 \equiv 0$, $3571 \equiv 0$, $9349 \equiv 0$,...

à l'aide des calculs suivants que nous ne faisons qu'indiquer :

$$
\begin{array}{lllll}
1^\circ & \varepsilon^2 + \varepsilon^3 \equiv 3, & \varepsilon^3 - \varepsilon^2 \equiv 4 & : 2\varepsilon^3 \equiv 7, & 2\varepsilon^2 \equiv -1, 4 \equiv -7; \\
2^\circ & \varepsilon^4 + \varepsilon^3 \equiv 7, & \varepsilon^3 - \varepsilon^4 \equiv 4 & : 2\varepsilon^3 \equiv 11, & 2\varepsilon^4 \equiv 3, 4 \equiv 33; \\
3^\circ & \varepsilon^6 + \varepsilon^5 \equiv 18, & \varepsilon^5 - \varepsilon^6 \equiv 11 & : 2\varepsilon^5 \equiv 29, & 2\varepsilon^6 \equiv 7, 4 \equiv 203; \\
4^\circ & \varepsilon^6 + \varepsilon^7 \equiv 18, & \varepsilon^7 - \varepsilon^6 \equiv 29 & : 2\varepsilon^7 \equiv 47, & 2\varepsilon^6 \equiv -11, 4 \equiv -517; \\
5^\circ & \varepsilon^8 + \varepsilon^9 \equiv 47, & \varepsilon^9 - \varepsilon^8 \equiv 76 & : 2\varepsilon^9 \equiv 123, & 2\varepsilon^8 \equiv -29, 4 \equiv -3567; \\
6^\circ & \varepsilon^{10} + \varepsilon^9 \equiv 123, & \varepsilon^9 - \varepsilon^{10} \equiv 76 & : 2\varepsilon^9 \equiv 199, & 2\varepsilon^{10} \equiv 47, 4 \equiv 9353;
\end{array}
$$

.....

2. Si on a formé les puissances impaires de $\varepsilon^1 - \varepsilon^{-1} \equiv 1$, on pourra combiner les résultats avec cette même relation, que l'on peut multiplier par $\varepsilon^{\frac{\varphi-1}{2}}$ et mettre sous la forme $\varepsilon^{\frac{\varphi+1}{2}} - \varepsilon^{\frac{\varphi-1}{2}} \equiv \varepsilon^{\frac{\varphi-3}{2}}$, de manière à obtenir ainsi $\varepsilon^{\frac{\varphi-3}{2}} \equiv e$; et, si on avait formé les puissances paires, on en combinerait les résultats avec la relation $\varepsilon^{\frac{\varphi-1}{2}} + \varepsilon^{\frac{\varphi+1}{2}} \equiv \varepsilon^{\frac{\varphi+3}{2}}$, déduite également de $\varepsilon^1 - \varepsilon^{-1} \equiv 1$ multiplié par $\varepsilon^{\frac{\varphi+1}{2}}$, pour en obtenir $\varepsilon^{\frac{\varphi+3}{2}} \equiv e$. Cette valeur numérique de $\varepsilon^{\frac{\varphi-3}{2}}$ ou celle de $\varepsilon^{\frac{\varphi+3}{2}}$ servira à déterminer les deux puissances dont on a besoin pour éliminer ε avec l'une des formes $1 + \varepsilon \equiv \varepsilon^2$, $\varepsilon^{\varphi-1} + 1 \equiv \varepsilon$, $\varepsilon^{\varphi-2} + \varepsilon^{\varphi-1} \equiv 1$ de la proposée.

On pourrait encore éliminer directement à l'aide des deux formes $\varepsilon^{\frac{\varphi+1}{2}} - \varepsilon^{\frac{\varphi-1}{2}} \equiv \varepsilon^{\frac{\varphi-3}{2}}$, $\varepsilon^{\frac{\varphi-1}{2}} + \varepsilon^{\frac{\varphi+1}{2}} \equiv \varepsilon^{\frac{\varphi+3}{2}}$ et de la valeur numérique e obtenue pour $\varepsilon^{\frac{\varphi-3}{2}}$ ou $\varepsilon^{\frac{\varphi+3}{2}}$. En effet, la première forme $\varepsilon^{\frac{\varphi+1}{2}} - \varepsilon^{\frac{\varphi-1}{2}} \equiv \varepsilon^{\frac{\varphi-3}{2}}$ ayant donné, avec les puissances impaires de $\varepsilon^1 - \varepsilon^{-1} \equiv 1$, la valeur e de $\varepsilon^{\frac{\varphi-3}{2}}$, on en déduit $e\varepsilon^{-\frac{\varphi-3}{2}} \equiv 1$ ou $e\varepsilon^{\frac{\varphi+3}{2}} \equiv 1$; la seconde forme donne alors $e\varepsilon^{\frac{\varphi-1}{2}} + e\varepsilon^{\frac{\varphi+1}{2}} \equiv 1$, de sorte qu'il reste à éliminer avec $\varepsilon^{\frac{\varphi+1}{2}} - \varepsilon^{\frac{\varphi-1}{2}} \equiv e$. S'il s'agit de $\varepsilon^{\frac{\varphi+3}{2}} \equiv e$, obtenu à l'aide de la seconde forme $\varepsilon^{\frac{\varphi-1}{2}} + \varepsilon^{\frac{\varphi+1}{2}} \equiv \varepsilon^{\frac{\varphi+3}{2}}$ et des puissances paires de $\varepsilon^1 - \varepsilon^{-1} \equiv 1$, on en déduira $e\varepsilon^{\frac{\varphi-3}{2}} \equiv 1$; et l'on aura, pour éliminer, les deux relations $e\varepsilon^{\frac{\varphi+1}{2}} - e\varepsilon^{\frac{\varphi-1}{2}} \equiv 1$, $\varepsilon^{\frac{\varphi-1}{2}} + \varepsilon^{\frac{\varphi+1}{2}} \equiv e$.

Mais il est plus commode de chercher le terme de la série qui contient la puissance de ε, dont on a obtenu la valeur numérique. Considérons, pour appliquer ce dernier mode d'élimination, le cas où l'on aurait formé les puissances impaires de $\varepsilon^1 - \varepsilon^{-1} \equiv 1$ (*); il suffira, pour obtenir les conditions numériques

$$11 \equiv 0,\quad 29 \equiv 0,\quad 199 \equiv 0,\quad 521 \equiv 0,\quad 3571 \equiv 0,\quad 9349 \equiv 0,\ldots$$

de multiplier entre elles les relations $\varepsilon^n \equiv e$, $\varepsilon^{\varphi-n} \equiv e'$, obtenues, comme il suit, pour chacune des valeurs de φ :

1° $\varepsilon^3 - \varepsilon^2 \equiv 4$, $\varepsilon^3 - \varepsilon^2 \equiv \varepsilon$: $\varepsilon \equiv 4$; mais $\varepsilon - \varepsilon^4 \equiv 1$: donc $\varepsilon^4 \equiv 3$;
2° $\varepsilon^3 - \varepsilon^4 \equiv 4$, $\varepsilon^4 - \varepsilon^3 \equiv \varepsilon^2$: $\varepsilon^2 \equiv -4$; mais $\varepsilon^5 - \varepsilon^2 \equiv 11$: donc $\varepsilon^5 \equiv 7$;
3° $\varepsilon^5 - \varepsilon^6 \equiv 11$, $\varepsilon^6 - \varepsilon^5 \equiv \varepsilon^4$: $\varepsilon^4 \equiv -11$; mais $\varepsilon^7 - \varepsilon^4 \equiv 29$: donc $\varepsilon^7 \equiv 18$;
4° $\varepsilon^7 - \varepsilon^6 \equiv 29$, $\varepsilon^7 - \varepsilon^6 \equiv \varepsilon^5$: $\varepsilon^5 \equiv 29$; mais $\varepsilon^5 - \varepsilon^9 \equiv 11$: donc $\varepsilon^8 \equiv 18$;
5° $\varepsilon^9 - \varepsilon^8 \equiv 76$, $\varepsilon^9 - \varepsilon^8 \equiv \varepsilon^7$: $\varepsilon^7 \equiv 76$; mais $\varepsilon^7 - \varepsilon^{10} \equiv 29$: donc $\varepsilon^{10} \equiv 47$;
6° $\varepsilon^9 - \varepsilon^{10} \equiv 76$, $\varepsilon^{10} - \varepsilon^9 \equiv \varepsilon^8$: $\varepsilon^8 \equiv -76$; mais $\varepsilon^{11} - \varepsilon^8 \equiv 199$: donc $\varepsilon^{11} \equiv 123$;
. . . . . .

(*) Cette série a été donnée à la page 8.

3. Enfin, toute relation de la forme $\varepsilon^u \equiv e$ donnant $e^\varphi \equiv 1$, il est clair que cette condition peut servir à donner directement les seuls facteurs qui échappent à la démonstration, quand il en existe. Or, comme on vient de le voir, on peut obtenir deux valeurs de e, à l'aide de $\varepsilon^{\frac{\varphi-3}{2}}$ et de $\varepsilon^{\frac{\varphi+3}{2}}$. Mais, la décomposition en facteurs présentant des difficultés aussitôt que les nombres $e^\varphi - 1$ deviennent considérables, on peut démontrer l'impossibilité de $e^\varphi \equiv 1$ pour certaines valeurs de θ, sans qu'il soit nécessaire de diviser $e^\varphi - 1$ par ces valeurs. Supposons d'abord e positif; on cherchera, à l'aide du procédé de Legendre rappelé dans notre troisième mémoire, le résidu de $e^{k\varphi n}$ relativement à θ. Si ce résidu est -1, la condition $e^\varphi \equiv 1$ sera absurde. Supposons maintenant que e soit négatif; la condition numérique devient $e'^\varphi \equiv -1$: si donc le résidu de $e'^{k\varphi n}$ est -1 et que k soit pair, ou si le résidu est 1 et que k soit impair, l'impossibilité sera encore manifeste (*). On voit que, si φ et n sont donnés *à priori*, on pourra, en faisant varier k, chercher une suite de valeurs θ pour lesquelles la condition numérique est impossible.

Cinquième note (**). On déduit en effet de $a\varepsilon^u + b\varepsilon^{-u} \equiv c\varepsilon^{2u}$, par les mêmes moyens, $a'\varepsilon^{3u} + b'\varepsilon^{-3u} \equiv c'\varepsilon^{6u} + d'$; et, si on carre ces deux relations plusieurs fois de suite, on trouve des résultats de la forme

$$A\varepsilon^{2^k u} + B\varepsilon^{-2^k u} \equiv C\varepsilon^{2^k u} + D\,; \quad A'\varepsilon^{2^k.3u} + B'\varepsilon^{-2^k.3u} \equiv C'\varepsilon^{2^k.6u} + D'.$$

Les exposants dans le premier membre étant numériquement de la forme $2^k u$, $2^k.3u$, et se réduisant aux restes de leur division par φ, se reproduisent à partir de $2^h = m\varphi + 1$, si nous désignons par h la plus petite puissance de 2 pour laquelle 1 soit résidu; car les puissances de 2, divisées par φ, ne peuvent donner deux restes égaux, si l'une d'elles n'a déjà donné 1 pour reste. Ainsi, dans chaque série, la relation de l'ordre

(*) Ces deux cas se ramènent d'ailleurs l'un à l'autre : il suffira de poser $e \equiv -e'$ si e est positif, et $e \equiv e'$ si e est négatif.

(**) Voir à la page 10.

$h+1$ aura les mêmes exposants que la première. Si $h=2h'$, on aura $2^{h'}=m\varphi-1$, et alors les relations de l'ordre $h'+1$ auront dans le premier membre les mêmes exposants que les premières, mais avec un signe contraire.

Enfin il se trouvera, dans les deux séries, des relations dans lesquelles les exposants de ε, considérés dans le premier membre, auront les mêmes valeurs numériques, toutes les fois que 3 ou -3 sera résidu d'une puissance de 2 divisée par φ, ou, ce qui revient au même, toutes les fois que 1 ou -1 sera, pour le même facteur φ, résidu d'une puissance de 2 multipliée par 3. C'est en effet le résultat auquel conduisent les égalités $2^k u=m\varphi\pm 2^{k'}.3u$ qui donnent $2^{k-k'}\equiv\pm 3$ et $2^{k'-k}.3\equiv\pm 1$, relativement à φ. Ces conditions ne peuvent avoir lieu l'une sans l'autre, parce que, si $2^m.3\equiv\pm 1$ et que $2^l\equiv 1$, relativement à φ, on a $2^m.3\equiv\pm 2^l$ et, par suite, $2^{l-m}\equiv\pm 3$. Réciproquement, si on avait $2^{m'}\equiv\pm 3$, on aurait $3.2^l\equiv\pm 2^{m'}$ et $3.2^{l-m'}\equiv\pm 1$.

Sixième note (*). Pour éviter d'avoir à vérifier que 14249 est *premier*, on peut avoir une autre relation.

En effet $1+\varepsilon\equiv-\varepsilon^3$ donne $\varepsilon^8+\varepsilon^9\equiv-\varepsilon^{11}$; d'où, en carrant, on obtiendra $\varepsilon^5\equiv 2+\varepsilon+\varepsilon^{16}$, et, par conséquent, $-\varepsilon^{15}\equiv\varepsilon^5-2$, ce qui conduit à $\varepsilon^{12}+\varepsilon^5\equiv 2\varepsilon^7$. Cette dernière relation donnerait une série qui suffirait pour éliminer ε; mais nous en obtenons à l'instant une seconde, à l'aide du moyen déjà indiqué. Il suffit en effet de cuber cette relation, ce qui donne $\varepsilon^2+\varepsilon^{15}\equiv 8\varepsilon^4-6\varepsilon^7$, et d'éliminer ε^7 avec $6\varepsilon^7+6\equiv 12\varepsilon^2$, pour trouver $13\varepsilon^2+\varepsilon^{15}\equiv 8\varepsilon^4+6$ qui servirait à former cette seconde série. Toutefois, comme on a déjà (page 10, 1re série) la relation $\varepsilon^2+\varepsilon^{15}\equiv\varepsilon^{13}-2$, l'élimination avec $13\varepsilon^2+\varepsilon^{15}\equiv 8\varepsilon^4+6$ ou $13+\varepsilon^{13}\equiv 8\varepsilon^2+6\varepsilon^{15}$ se présente d'elle-même, et l'on a $15-5\varepsilon^{15}\equiv 7\varepsilon^2$ ou $15\varepsilon^{15}-5\varepsilon^{13}\equiv 7$; mais $5\varepsilon^2+5\varepsilon^{15}\equiv 5\varepsilon^{13}-10$: donc $10\varepsilon^{15}-5\varepsilon^2\equiv 17$. Éliminant entre cette dernière et $5\varepsilon^{15}+7\varepsilon^2\equiv 15$, on trouve successivement $19\varepsilon^2\equiv 13$, $95\varepsilon^{15}\equiv 194$, $1805\equiv 2522$, et, par conséquent, $717\equiv 0$. Or $717=3.239$.

(*) Voir à la page 12.

Septième note (*). Voici un moyen particulier qui donne directement la condition numérique $613 \equiv 0$, de manière à éviter la considération du nombre 153991.

Ajoutons d'abord membre à membre les relations suivantes, qui se déduisent toutes de la première d'entre elles :

$$\varepsilon^2 + 1 \equiv \varepsilon^{16}, \quad \varepsilon - \varepsilon^4 \equiv \varepsilon^2, \quad \varepsilon^{15} - \varepsilon \equiv \varepsilon^{16}, \quad \varepsilon^{14} \equiv \varepsilon^{15} + 1, \quad 2\varepsilon^{14} + 2\varepsilon^{16} \equiv 2\varepsilon^{13};$$

nous trouvons, après réduction, $3\varepsilon^{14} - \varepsilon^4 \equiv 2\varepsilon^{13}$, d'où l'on forme :

$$2\varepsilon^9 - 3\varepsilon^9 \equiv -\varepsilon^{16}, \quad 4\varepsilon^{16} + 9\varepsilon \equiv \varepsilon^{15} + 12, \quad 3\varepsilon^{16} + 8\varepsilon \equiv 12.$$

On pourrait déjà combiner le dernier de ces résultats avec $453\varepsilon \equiv -7$, ce qui donnerait $654071 \equiv 0$ ou $11.97.613 \equiv 0$. Mais, si on continue les transformations, on trouve $3\varepsilon^{15} + 8 \equiv 12\varepsilon^{16}$, $3\varepsilon + 8 \equiv 9\varepsilon^{16}$; et, comme $9\varepsilon^{16} + 24\varepsilon \equiv 36$, à cause de $3\varepsilon^{16} + 8\varepsilon \equiv 12$, on obtient $27\varepsilon \equiv 28$, $81\varepsilon^{16} \equiv 100$, et, par conséquent, $2187 \equiv 2800$, c'est-à-dire $613 \equiv 0$.

Huitième note. A ne considérer que les nombres au-dessus de 101, voici les nombres que nous avons laissé au lecteur le soin de vérifier comme *premiers* (page 18) :

2e principe.		199,	521,	3571,	9349;		
3e principe.		607,	239,	14249,	137,	457,	919;
4e principe.	1°	173,	137,	5483,	2741,	229,	347;
	2°	103,	7109,	1777,	191,	599;	
	3°	131,	613,	153991,	1483.		

Il faut leur ajouter les deux nombres 4093 et 7541 de la première note (page 19).

(*) Voir à la page 17.

FIN DU SECOND LIVRE DE LA PREMIÈRE PARTIE.

Paris. — Typographie de Firmin Didot frères, rue Jacob, 56.

CINQUIÈME MÉMOIRE

SUR

LA THÉORIE DES NOMBRES,

PAR M. F. LANDRY,

LICENCIÉ ÈS SCIENCES MATHÉMATIQUES.

Juillet 1856.

BODL. BIBLIOTH.

THÉORÈME

SUR LES RÉDUITES D'UNE NOUVELLE ESPÈCE DE FRACTIONS CONTINUES.

PARIS,

LIBRAIRIE DE L. HACHETTE ET Cie,

RUE PIERRE-SARRASIN, N° 14,

(Près de l'École de médecine).

1856.

Le troisième et dernier livre de la première partie des *Recherches nouvelles* sur le théorème de Fermat, paraîtra *très-incessamment*.

THÉORÈME

SUR LES RÉDUITES D'UNE NOUVELLE ESPÈCE DE FRACTIONS CONTINUES.

QUELQUES MOTS AU SUJET DU NOUVEAU THÉORÈME.

Dans leurs recherches sur l'analyse indéterminée, les géomètres ont fait dépendre la résolution des questions qu'ils ont abordées, de celle d'équations qui sont devenues célèbres dans la science; et les principes, qu'ils ont posés, sont restés comme les bases de la théorie. Telles sont surtout les équations $x^2 - Ay^2 = \pm 1$, $x^2 - Ay^2 = \pm D$.

Nous proposons aujourd'hui un théorème qui a rapport à la résolution des équations de la forme $x^2 - Ay^2 = r^m$, dans le cas particulier de $A + r = a^2$, et qui par conséquent peut servir à donner une infinité de solutions pour $x^2 - Ay^2 = z^m$, puisqu'il suffit de prendre $z + A$ égal à un carré quelconque.

Les équations de cette forme sont, il est vrai, comprises dans la seconde des équations générales ci-dessus mentionnées, mais leur résolution par les méthodes connues donnerait lieu à de longs calculs, même dans les cas les moins compliqués.

D'ailleurs, malgré la fécondité parfois téméraire de Fermat (*), il ne

(*) Fermat avait annoncé que, si l'on prenait pour x l'un des nombres de la progression 1, 2, 4, 8..., etc., la formule $2^x + 1$ donnait toujours des nombres *premiers*. Suivant une remarque d'Euler, rapportée par Legendre, cette assertion est fausse.

nous a pas paru que l'analyse fût assez riche en propositions *délectables*, comme les appelaient nos pères, pour qu'il n'y eût pas à regretter l'omission d'une propriété à la fois élégante et simple.

Nous croyons de plus que le nouveau développement *continu* de $\sqrt{A}$, sur lequel nous nous appuyons, peut conduire à d'utiles applications; et, pour en citer une, il constitue un procédé d'approximation dans le calcul de la racine carrée d'un nombre. Les *réduites* de ce développement donnent, en effet, les valeurs approchées que l'on cherche, avec une grande rapidité, une fois que l'on a déterminé une partie importante de la racine (*)

Enfin notre théorème démontre la possibilité de représenter d'une infinité de manières, sous la forme du second degré $x^2 - Ay^2$, une puissance quelconque m d'un nombre donné r. Il suffit, en effet, de prendre A de telle sorte que $A + r$ soit égal à un carré. Cette dernière considération avait singulièrement éveillé notre attention par l'espoir d'en tirer parti pour la démonstration du théorème de Fermat; mais nous n'avons pu réussir encore à en obtenir rien de bien remarquable, ce qui nous a engagé à poursuivre les recherches que nous avons faites dans une autre voie, et dont nous avons déjà publié deux livres.

(*) Les méthodes, qui se rapportent à l'extraction de la racine carrée des nombres, ont, au point de vue pratique, un intérêt que n'ont pas les méthodes d'extraction, lorsqu'il s'agit de racines d'un degré plus élevé, parce que les procédés logarithmiques, qui s'appliquent avec tant de succès à l'extraction des racines des nombres en général, ne donnent pas toujours, pour les racines carrées en particulier, du moins avec les tables en usage, l'approximation qui convient aux questions un peu délicates, approximation d'ailleurs incertaine et mal définie.

NOUVELLE ESPÈCE DE FRACTIONS CONTINUES.

Le développement, que Lagrange a donné de $\sqrt{A}$, peut être présenté sous une autre forme, et de cette seconde forme découle presque immédiatement le théorème que nous avons à exposer.

Voici ce développement :

Soit $A = a^2 + r$, on a

$$\sqrt{A} = a + \sqrt{A} - a, \text{ ou } \sqrt{A} = a + \frac{(\sqrt{A} - a)(\sqrt{A} + a)}{\sqrt{A} + a}, \text{ et } \sqrt{A} = a + \frac{r}{\sqrt{A} + a}.$$

Si, dans le second membre de cette expression, on remplace $\sqrt{A}$ par le second membre lui-même, et que l'on continue ainsi dans les valeurs successives que l'on obtient pour le premier membre de l'égalité, on trouve

$$\sqrt{A} = a + \cfrac{r}{2a + \cfrac{r}{2a + \cfrac{r}{2a + \text{etc.}}}}$$

Cette nouvelle espèce de fractions *continues* ne diffère de celles que tout le monde connaît, que parce que le dénominateur incomplet des fractions *intégrantes* est constant, et que le numérateur de ces mêmes fractions, bien que constant lui-même, n'est pas nécessairement égal à l'unité.

Les *réduites* se forment d'après une loi facile à démontrer. On voit, en effet, qu'avec deux *réduites* consécutives $\frac{m}{m'}$, $\frac{n}{n'}$, on formera la suivante $\frac{p}{p'}$, en prenant $p = 2na + mr$, $p' = 2n'a + m'r$.

Si donc a^2 est un carré approché de A, les *réduites* de la fraction *continue* seront des valeurs de plus en plus approchées de $\sqrt{A}$ (*).

Nous laissons de côté ces considérations, du genre le plus élémentaire, pour arriver au théorème,

(*) Il est évident que, si $A = a^2 + r$, $\sqrt{A}$ est compris entre a et $a + \frac{r}{2a}$, quel que soit le signe de r. Voir la première note, page 10.

THÉORÈME

Sur les réduites des nouvelles fractions *continues*.

Soit $\frac{m}{m'}$, une *réduite* de l'ordre u; je dis que l'on aura $m^2 - Am'^2 = r^u$, ou $m^2 - Am'^2 = -r^u$, suivant que u sera un nombre pair ou un nombre impair. Cette loi se vérifie immédiatement sur les premières *réduites*. Il est d'ailleurs évident que, si r était *négatif*, on n'aurait plus qu'un signe, et que l'égalité serait $m^2 - Am'^2 = r^u$, quel que fût le nombre entier u.

Tel est le principe qui nous a frappé.

Pour en démontrer la généralité, considérons les *réduites* consécutives

$$\frac{l}{l'}, \quad \frac{m}{m'}, \quad \frac{n}{n'}, \quad \frac{p}{p'};$$

et supposons la loi démontrée jusqu'à $\frac{p}{p'}$ exclusivement.

Des valeurs $n = 2ma + lr$, $n' = 2m'a + l'r$, il résulte :

$$n^2 - An'^2 = 4a^2(m^2 - Am'^2) + 4ar(lm - Al'm') + r^2(l^2 - Al'^2);$$

et, comme on a, par hypothèse, $n^2 - An'^2 = r^2(l^2 - Al'^2)$, il faut que l'on ait $a(m^2 - Am'^2) + r(lm - Al'm') = 0$.

Cela posé, à l'aide des valeurs $p = 2na + mr$, $p' = 2n'a + m'r$, on trouvera

$$p^2 - Ap'^2 = 4a^2(n^2 - An'^2) + 4ar(mn - Am'n') + r^2(m^2 - Am'^2),$$

résultat qui devient, si l'on remplace n et n' par leurs valeurs dans le second terme du second membre,

$$p^2 - Ap'^2 = 4a^2(n^2 - An'^2) + 8a^2r(m^2 - Am'^2) + 4ar^2(lm - Al'm') + r^2(m^2 - Am'^2).$$

Les trois premiers termes du second membre de cette égalité, pouvant se mettre sous la forme

$$4a^2[(n^2 - An'^2) + r(m^2 - Am'^2)] + 4ar[a(m^2 - Am'^2) + r(lm - Al'm')],$$

se réduisent à zéro, à cause de

$$n^2 - An'^2 + r(m^2 - Am'^2) = 0, \quad \text{et de} \quad a(m^2 - Am'^2) + r(lm - Al'm') = 0:$$

il reste donc $p^2 - Ap'^2 = r^2(m^2 - Am'^2)$.

En conséquence, si $m^2 - Am'^2 = \pm r^{u-2}$, on aura $p^2 - Ap'^2 = \pm r^u$, ce qui démontre la loi.

Cette démonstration est celle qui se présente la première à l'esprit; mais en voici une autre qui nous paraît beaucoup plus simple.

Considérons les mêmes *réduites* $\frac{m}{m'}$, $\frac{n}{n'}$, $\frac{p}{p'}$, dont la dernière a pour expression

$$\frac{p}{p'} = \frac{2na + mr}{2n'a + m'r};$$

et désignons par y la valeur $\sqrt{A} + a$, dénominateur complet dont $2a$ n'est qu'une valeur approchée; nous aurons

$$\sqrt{A} = \frac{ny + mr}{n'y + m'r},$$

d'où l'on déduira

$$(n^2 - An'^2)y^2 + 2r(mn - Am'n')y + r^2(m^2 - Am'^2) = 0.$$

Mais de $y - a = \sqrt{A}$ on déduit également $y^2 - 2ay - r = 0$. En conséquence, puisque les deux équations ont les mêmes racines, on doit avoir

$$r\frac{mn - Am'n'}{n^2 - An'^2} = -a, \quad \text{et} \quad r^2\frac{m^2 - Am'^2}{n^2 - An'^2} = -r:$$

or cette dernière égalité donne

$$n^2 - An'^2 = -r(m^2 - Am'^2).$$

Ainsi, pour passer d'un résultat $m^2 - Am'^2$ au suivant $n^2 - An'^2$, il faut multiplier le premier par $-r$.

APPLICATIONS.

Nous nous bornerons à quelques réflexions.

D'abord la règle est facile à saisir, et peut se présenter comme il suit.

Supposons que l'on ait $A = a^2 + r$, r représentant un nombre *positif*, le développement sera

$$\sqrt{A} = a + \cfrac{r}{2a + \cfrac{r}{2a + \text{etc.}}};$$

et la réduite $\frac{m}{m'}$ de l'ordre u donnera $x = \pm m$, $y = \pm m'$ pour résoudre $x^2 - Ay^2 = r^u$, lorsque le nombre u sera pair, ou $x^2 - Ay^2 = -r^u$, lorsque le nombre u sera impair.

Mais, si l'on a $A = a^2 - r$, le développement sera

$$\sqrt{A} = a - \cfrac{r}{2a - \cfrac{r}{2a - \text{etc.}}};$$

et l'on aura $x = \pm m$, $y = \pm m'$ pour résoudre $x^2 - Ay^2 = r^u$, u étant égal au rang de la *réduite* $\frac{m}{m'}$.

Il suffit de faire attention à la forme de l'équation $x^2 - Ay^2 = \pm r^u$, pour comprendre que x et y ne peuvent avoir d'autres diviseurs *premiers* communs que ceux de r. D'un autre côté, il résulte de la loi de formation des termes des *réduites*, que ces termes ne peuvent avoir d'autres facteurs *premiers* communs, diviseurs de r, que ceux communs à r et à $2a$ (*). Il faut donc conclure de ces observations et de la condition $A = a^2 \pm r$, que les valeurs trouvées par notre méthode pour x et y, ne sauraient avoir d'autres diviseurs *premiers* communs, 2 excepté, que ceux communs à r et à A. En conséquence, toutes les fois que r sera *premier* avec A, les valeurs dont nous parlons seront *premières* entre elles si r est impair, et, s'il est pair, elles ne pourront avoir pour commun diviseur qu'une puissance de 2.

On peut appliquer aux exemples suivants :

$$x^2 - 29y^2 = 7^3; \quad x^2 - 19y^2 = 3^4; \quad x^2 - 31y^2 = -6^3;$$

et l'on trouvera, respectivement (**),

$x = \pm 738$, $y = \pm 137$; $x = \pm 2441$, $y = \pm 560$; $x = \pm 590$, $y = \pm 106$.

Les solutions, ainsi obtenues, ne sont pas les seules que l'on puisse trouver par notre méthode. Nous les appellerons indépendantes de r, pour les distinguer de celles dont nous allons parler, et qui ont pour facteur commun une puissance de r.

Posons $x = r^v x'$, $y = r^v y'$, $2v$ étant moindre que $u + 1$; l'équation $x^2 - Ay^2 = \pm r^u$ deviendra, après la suppression du facteur commun r^{2v}, $x'^2 - Ay'^2 = \pm r^{u-2v}$; et, si l'on résout cette dernière équation, les valeurs

(*) En effet, pour former $\frac{p}{p'}$ à l'aide des *réduites* précédentes $\frac{n}{n'}$, $\frac{m}{m'}$, on a

$$p = 2na + mr, \qquad p' = 2n'a + m'r.$$

Ainsi on ne peut imaginer aucun diviseur *premier* de r, commun à p et à p', qui ne divise n et n', s'il ne divise $2a$. Or, divisant n et n', il diviserait l et l', puis h et h'... etc., et par conséquent les deux termes de la seconde *réduite* qui est $\frac{2a^2 + r}{2a}$.

(**) Voir, pour le calcul, la deuxième note, page 12.

de x', y', multipliées par r', résoudront la proposée. On fera donc successivement

$$v = 1, \quad v = 2, \quad v = 3, \quad \ldots \quad v = \frac{u-2}{2} \text{ ou } v = \frac{u-1}{2},$$

suivant que u sera un nombre pair ou un nombre impair, et les solutions se déduiront des *réduites,* dont le rang est indiqué par les nombres

$$u-2, \quad u-4, \quad u-6, \quad \ldots \quad 3 \text{ ou } -1.$$

Il suffira, pour les obtenir, de multiplier les deux termes de ces *réduites,* respectivement, par les facteurs

$$r, \quad r^2, \quad r^3, \quad \ldots \quad r^{\frac{u-2}{2}} \text{ ou } r^{\frac{u-1}{2}}.$$

Si u était un nombre pair, et qu'on voulût trouver les solutions de la forme $x = r^{\frac{u}{2}}x'$, $y = r^{\frac{u}{2}}y'$, on aurait à résoudre l'équation $x'^2 - Ay'^2 = \pm 1$.

Enfin, pour trouver des nombres entiers qui résolvent l'équation $x^2 - Ay^2 = z^m$, on prendra pour z l'une quelconque des valeurs déterminées par la relation $A = a^2 - z$, et l'on cherchera x et y par la méthode précédente. On pourra même prendre $A = a^2 + z$, si m est pair; mais, s'il s'agit de résoudre $x^2 - Ay^2 = -z^m$, il faudra d'abord que m soit impair, et l'on devra poser $A = a^2 + z$.

Nous terminons ce très-mince opuscule en faisant observer que notre théorie n'exclut aucune valeur *positive* de A qui peut être un carré parfait (*). Il resterait, il est vrai, à montrer comment chacune des solutions que nous venons d'enseigner à obtenir pour $x^2 - Ay^2 = r^m$, ou pour $x^2 - Ay^2 = -r^m$, peut, lorsque A n'est pas un carré parfait, servir à former une série infinie de solutions *semblables;* mais, sur ce point, nous renvoyons aux notes qui suivent (**), et aux ouvrages de Legendre et de Gauss.

(*) Les auteurs ont considéré à part le cas où A est un carré parfait a^2. On procède alors à la résolution, par la décomposition en facteurs, ce qui conduit à deux équations du premier degré, $x - ay = \theta$, $x + ay = \frac{D}{\theta}$, θ étant un diviseur quelconque de D, qui ne surpasse pas $\sqrt{D}$. Il reste à prendre, s'il est possible, ce diviseur θ, de manière que x et y soient entiers.

(**) Voir la troisième note, page 13.

NOTES DU CINQUIÈME MÉMOIRE.

PREMIÈRE NOTE (*).

Principes sur les nouvelles fractions continues. — Application.

Si on considère la forme générale du développement

$$a + \cfrac{r}{2a + \cfrac{r}{2a + \text{etc.},}}$$

et les *réduites* consécutives d'un ordre quelconque $\frac{m}{m'}$, $\frac{n}{n'}$, $\frac{p}{p'}$, on trouve pour les différences de ces *réduites*,

$$\frac{m}{m'} - \frac{n}{n'} = \frac{mn' - nm'}{m'n'}, \qquad \frac{n}{n'} - \frac{p}{p'} = \frac{np' - pn'}{n'p'}.$$

Mais, à cause des valeurs de p et de p', on a $np' - pn' = (nm' - mn')r$, c'est-à-dire que les numérateurs des différences se forment les uns des autres : il suffit, pour les former, de multiplier par $-r$ celui qui précède immédiatement.

Or, si on soustrait la seconde *réduite* $\frac{2a^2 + r}{2a}$ de la première $\frac{a}{1}$, le numérateur de la différence est $-r$; donc les numérateurs suivants seront r^2, $-r^3$, ... etc.; de sorte que, si l'on cherche la différence entre la *réduite* de l'ordre u et celle qui la suit immédiatement, le numérateur de cette différence sera r^u ou $-r^u$, suivant que le nombre u sera pair ou impair (**).

Cela posé, comme, dans l'hypothèse de $A = a^2 + r$, quel que soit le signe de r, la valeur de $\sqrt{A}$ est toujours comprise entre deux *réduites* consécutives, si on prend la *réduite* $\frac{p}{p'}$ de l'ordre u pour la valeur de $\sqrt{A}$, l'erreur commise sera moindre que $\frac{r^u}{n'p'}$, et, à plus forte raison, que $\frac{r^u}{n'^2}$. Il résulte de là un moyen simple pour trouver une limite du degré d'approximation que l'on obtient, lorsque, dans le calcul de $\sqrt{A}$, on s'arrête à une *réduite* de l'ordre u.

(*) Cette note a été annoncée à la page 5.

(**) Il faut cependant faire cette restriction que les *réduites* n'auront pas été simplifiées.

Mais, si l'on veut connaître approximativement dans quel rapport varie, d'une *réduite* à l'autre, cette limite de l'erreur commise, il suffit, pour s'en rendre compte, de comparer deux différences successives dont les valeurs, abstraction faite du signe, sont

$$\frac{mn' - m'n}{m'n'}, \qquad \frac{(mn' - m'n)\,r}{n'p'};$$

et l'on voit que, pour passer de l'une à l'autre, il faut multiplier la première par $\frac{m'r}{p'}$ ou $\frac{m'r}{2an' + m'r}$, qui est la même chose que $\frac{m'r}{4a^2m' + 2ar + m'r}$. Cette dernière expression, étant moindre que $\frac{r}{4a^2}$, est inférieure à $\frac{1}{2a}$, puisque r est au plus égal à $2a$ (*).

Ainsi on pourra connaître, dans chaque cas, l'utilité qu'il y aurait à prendre une *réduite* de plus, et l'on pourra même décider, à l'avance, suivant le degré d'approximation réclamé par la question, l'ordre de la *réduite* à laquelle il convient de s'arrêter.

Il est clair que la méthode pour trouver $\sqrt{A}$, lorsque l'on part de $A = a^2 + r$, offrira d'autant plus d'avantage que r sera petit relativement à a.

Proposons-nous de chercher la racine carrée de 31, en prenant $31 = 25 + 6$, bien qu'il fût préférable, pour la rapidité du calcul, de prendre $31 = 36 - 5$; on a aussitôt

$$\sqrt{31} = 5 + \cfrac{6}{10 + \cfrac{6}{10 + \text{etc.}}};$$

et, si l'on fait abstraction de la partie entière, on trouve pour les *réduites :*

$$\frac{6}{10}; \quad \frac{60}{106}; \quad \frac{636}{1120}; \quad \frac{6720}{11836}; \quad \frac{71016}{125080}; \quad \frac{750480}{1321816}\ldots; \text{ etc.}$$

dont les valeurs décimales sont respectivement

0,6; 0,566...; 0,56785...; 0,567759...; 0,5677646...; 0,567764348...; etc.

(*) Comme des deux carrés consécutifs qui comprennent le nombre A, on peut toujours choisir celui des deux qui donne le moindre reste r, ce dernier sera moindre que $a + 1$, puisque la somme des deux restes est $2a + 1$. Avec cette attention, $\frac{r}{4a^2}$ ne saurait excéder $\frac{1}{4a}$.

Mais, si l'on prend un chiffre décimal de plus, et qu'on pose $a = 5{,}5$, on trouvera le développement

$$\sqrt{31} = 5{,}5 + \cfrac{0{,}75}{11 + \cfrac{0{,}75}{11 + \text{etc.}}},$$

dont les *réduites*, abstraction faite de a, sont

$$\frac{75}{1100}; \qquad \frac{825}{12175}; \qquad \frac{913125}{13475000}.$$

Si on les convertit en décimales, et qu'on leur ajoute 5,5, on obtient, pour $\sqrt{31}$, les valeurs approchées

5,568 ; 5,567761 ; 5,56776437.

Enfin, en prenant encore, pour a, un chiffre décimal de plus, on a

$$\sqrt{31} = 5{,}56 + \cfrac{0{,}0864}{11{,}12 + \cfrac{0{,}0864}{11{,}12 + \text{etc.}}},$$

et l'on trouve les *réduites*

$$\frac{864}{111200}, \qquad \frac{960768}{12374080 0}, \ldots$$

dont les valeurs décimales, augmentées de 5,56, sont

5,567769... ; 5,56776436 7....

Le calcul par logarithmes, avec les tables de Callet, donne, pour cette racine de 31, la valeur approchée 5,5677647, dont le septième chiffre décimal est inexact; encore faut-il faire une division pour trouver les trois derniers chiffres, car les tables ne donnent que cinq chiffres.

Les tables à cinq décimales de Reynaud donnent 5,56775, valeur inexacte au cinquième chiffre décimal, et dont les deux derniers chiffres ont nécessité une division.

DEUXIÈME NOTE (*).

Détail du calcul précédemment annoncé.

1er EXEMPLE : $x^2 - 29y^2 = 7^2$, $\sqrt{29} = 6 - \cfrac{7}{12 - \cfrac{7}{12 - \text{etc.}}}$

Réduites : $\frac{6}{1}$, $\frac{65}{12}$, $\frac{738}{137}$.

(*) Cette note a été indiquée à la page 8.

2e EXEMPLE : $x^2 - 19y^2 = 3^4$, $\sqrt{19} = 4 + \cfrac{3}{8 + \cfrac{3}{8 + \text{etc.}}}$

Réduites : $\frac{4}{1}$, $\frac{35}{8}$, $\frac{292}{67}$, $\frac{2441}{560}$.

3e EXEMPLE : $x^2 - 31y^2 = -6^3$, $\sqrt{31} = 5 + \cfrac{6}{10 + \cfrac{6}{10 + \text{etc.}}}$

Réduites : $\frac{5}{1}$, $\frac{56}{10}$, $\frac{590}{106}$.

Les solutions dépendantes de r, obtenues par le même calcul, seraient

pour le premier exemple..... $x = \pm 7.6$, $y = \pm 7.1$;
pour le deuxième exemple..... $x = \pm 3.35$; $y = \pm 3.8$;
et pour le troisième..... $x = \pm 6.5$, $y = \pm 6.1$.

TROISIÈME NOTE (*).

Résumé des méthodes de Lagrange et de Gauss. — Observation importante. Application de ces méthodes aux équations qui ont servi d'exemples.

Nous ne pouvons évidemment, ne fût-ce que pour la comparaison des procédés, quitter un pareil sujet, sans appliquer au cas particulier que nous avons traité, les méthodes générales données pour la résolution de l'équation $x^2 - Ay^2 = \pm D$, et dont nous sommes redevables au génie de Lagrange et de Gauss. Ces méthodes nous paraissent d'ailleurs connues de peu de personnes, bien que chacun s'imagine qu'elles le sont de tout le monde.

Nous nous bornerons au cas où les solutions sont des nombres *premiers* entre eux, tous les autres cas pouvant se ramener à celui-là. A est d'ailleurs un nombre *positif*, non carré (**).

MÉTHODE DE LAGRANGE.

Legendre, où nous trouvons la méthode de Lagrange, considère deux cas, celui de $D < \sqrt{A}$, et celui de $D > \sqrt{A}$. Nous les résumons de la manière suivante :

PREMIER CAS. On développe $\sqrt{A}$ en fraction *continue*, et les *réduites*

(*) Cette note a été annoncée à la page 9.

(**) Voir la petite observation au bas de la page 9.

qui correspondent aux quotients complets dont le dénominateur est D, fournissent des valeurs qui résolvent la proposée, de telle sorte que, si la *réduite* $\frac{p}{q}$ correspondant à un de ces quotients complets, est plus grande que $\sqrt{A}$, ses deux termes p et q satisfont à l'équation $x^2 - Ay^2 = D$; et que, si au contraire elle est moindre que $\sqrt{A}$, ses deux termes sont une solution de $x^2 - Ay^2 = -D$. Comme les *réduites* sont alternativement moindres ou plus grandes que $\sqrt{A}$, le rang d'une *réduite* suffit pour fixer les idées à cet égard.

Le développement de $\sqrt{A}$ en fraction *continue* étant toujours périodique, on doit développer l'étendue d'une période entière. S'il ne s'y trouve aucun quotient complet dont le dénominateur soit D, il ne s'en trouvera dans aucune autre période; et alors aucune des deux équations $x^2 - Ay^2 = \pm D$ ne sera résoluble. S'il s'en trouve un ou plusieurs, ce qui est possible dans le cas général, ces mêmes quotients se reproduiront dans toutes les périodes, et les *réduites* correspondantes fourniront ainsi une infinité de solutions, mais pouvant toutes se déduire des premières, respectivement, par une loi fort ingénieuse.

En effet, puisque A est un nombre entier non carré et *positif*, l'équation $\Phi^2 - A\Psi^2 = 1$ est toujours résoluble, d'une infinité de manières, par le simple développement de $\sqrt{A}$; et, si l'on appelle φ et ψ l'une de de ces solutions, celle des moindres nombres par exemple, toutes les autres se déduisent de celle-là, au moyen de la série *récurrente* (*)

(*) Cette série se reconnaît immédiatement, sans le développement du binôme, de la manière suivante :

Les équations $\Phi + \sqrt{A}\Psi = (\varphi + \sqrt{A}\psi)^m$, $\Phi - \sqrt{A}\Psi = (\varphi - \sqrt{A}\psi)^m$ donnent :

$$\Phi = \frac{(\varphi + \sqrt{A}\psi)^m + (\varphi - \sqrt{A}\psi)^m}{2}, \qquad \sqrt{A}\Psi = \frac{(\varphi + \sqrt{A}\psi)^m - (\varphi - \sqrt{A}\psi)^m}{2}.$$

Or l'expression $(\varphi + \sqrt{A}\psi)^m + (\varphi - \sqrt{A}\psi)^m$ peut être mise sous la forme

$$[(\varphi + \sqrt{A}\psi)^{m-1} + (\varphi - \sqrt{A}\psi)^{m-1}]\,[(\varphi + \sqrt{A}\psi) + (\varphi - \sqrt{A}\psi)]$$
$$- [(\varphi + \sqrt{A}\psi)^{m-2} + (\varphi - \sqrt{A}\psi)^{m-2}]\,(\varphi + \sqrt{A}\psi)\,(\varphi - \sqrt{A}\psi);$$

de sorte qu'en substituant Φ_μ à $\frac{(\varphi + \sqrt{A}\psi)^\mu + (\varphi - \sqrt{A}\psi)^\mu}{2}$, et réduisant, on trouve

$$\Phi_m = 2\varphi\Phi_{m-1} - \Phi_{m-2}.$$

On trouve de même $\qquad \Psi_m = 2\varphi\Psi_{m-1} - \Psi_{m-2}.$

$$\Phi + \sqrt{A}\Psi = (\varphi + \sqrt{A}\psi)^m,$$

de telle sorte que pour avoir Φ_1, Ψ_1; Φ_2, Ψ_2; Φ_3, Ψ_3;... etc., il suffit de faire successivement $m = 1$; $m = 2$; $m = 3$; ... etc. Les séries, qui donnent ces valeurs de Φ et de Ψ, ont, l'une et l'autre, pour *échelle de relation*, 2φ et -1.

Soit donc p et q une solution quelconque de $x^2 - Ay^2 = D$, ou de $x^2 - Ay^2 = -D$, on obtiendra toutes les solutions qui se rapportent périodiquement à celle-là, au moyen des formules générales

$$x = p\Phi \pm Aq\Psi, \qquad y = p\Psi \pm q\Phi,$$

dans lequelles le signe de Ψ peut être changé à volonté, et qui sont, du reste, faciles à vérifier par la simple substitution.

Deuxième cas. Dans l'hypothèse de $D > \sqrt{A}$, il faut recourir à la méthode générale donnée pour l'équation complète $Lx^2 + Mxy + Ny^2 = \pm D$ dans le cas particulier de $M^2 - 4LN = 4A$. On transforme cette équation, en posant $x = ny + Du$, et en prenant n de manière que $n^2 - A$ soit D ou un multiple de D. On la ramène ainsi pour chaque valeur de n comprise dans les limites de $-\frac{D}{2}$ à $\frac{D}{2}$, à la forme $ay^2 + byu + cu^2 = \pm 1$ que l'on résout en développant l'une des racines de $ay^2 + by + c = 0$ en fraction *continue*. Les *réduites* correspondant aux quotients complets dont le dénominateur est D, résolvent l'une ou l'autre des équations $ay^2 + byu + cu^2 = \pm D$, selon le rang de la *réduite*. Connaissant y et u, on en déduit facilement la valeur de x. Lorsque $M = 0$ dans la proposée, on n'a besoin de considérer que les valeurs *positives* de n, parce que les valeurs *négatives* conduiraient au développement des mêmes racines, et que les deux racines d'une équation du second degré donnent la même série.

Une fois que l'on aura déterminé une solution p, q, pour chaque valeur de n, de $-\frac{D}{2}$ à $\frac{D}{2}$, chacune de ces solutions servira à former une série de solutions *semblables* au moyen des formules

$$x = p\Phi \pm Aq\Psi, \qquad y = p\Psi \pm q\Phi;$$

ce qui dispense de développer la fraction *continue* au delà d'une période. Φ et Ψ représentent d'ailleurs, comme nous l'avons dit précédemment, les diverses solutions de $\Phi^2 - A\Psi^2 = 1$, et se déduisent d'une seule solution

φ, ψ, supposée connue, à l'aide de la relation $\Phi + \sqrt{A}\Psi = (\varphi + \sqrt{A}\psi)^m$, par la variation de m.

Il est clair que, s'il ne se trouvait aucune valeur de n, l'équation ne saurait être résolue.

MÉTHODE DE GAUSS.

La méthode appliquée à l'équation générale $ax^2 + 2bxy + cy^2 = D$, dans le cas de $b^2 - ac = A$, exige d'abord que D, quel que soit son signe, soit un *résidu quadratique* de A, c'est-à-dire que l'on puisse satisfaire à la condition $N^2 = D + At$. Si cette condition, qui revient du reste à celle que donne Lagrange pour la détermination de n dans le deuxième cas, n'est pas remplie, l'équation ne peut être résolue. Si elle est satisfaite, on cherche alors, pour chaque valeur de N, séparément, les valeurs de x et de y qui peuvent ramener la forme $ax^2 + 2bxy + cy^2$ à la forme $Dx^2 + 2Nxy + \frac{N^2 - A}{D}y^2$; et, si cette condition est satisfaite *proprement* (*) par $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$ les valeurs $x = \alpha$, $y = \gamma$ sont une solution de la proposée.

Dans l'application du procédé, on se borne aux valeurs de N *positives* ou *négatives*, qui numériquement ne sont pas supérieures à $\frac{D}{2}$. La transformation définitive s'obtient au moyen de transformations successives dont nous avons longtemps hésité à donner la règle, parce que nous désespérons de la donner avec une clarté suffisante.

Pour opérer ces transformations successives, on passe de la forme $ax^2 + 2bxy + cy^2$ ainsi représentée (a, b, c), suivant Gauss, à la forme (a', b', c'), en posant $b + b' = ha'$ et $c' = \frac{b'^2 - A}{a'}$, h devant être déterminé de telle sorte que b' soit compris entre $\sqrt{A}$ et $\sqrt{A} - a'$, si a' est *positif*, ou entre $\sqrt{A}$ et $\sqrt{A} + a'$, si a' est *négatif*. On continue ainsi, de forme en forme, jusqu'à ce qu'on en trouve une, ce qui arrive infailliblement, dans laquelle le troisième terme ne soit pas plus petit que le premier, et qui prend le nom de forme *réduite*, dans la langue de Gauss.

(*) Expression de Gausse qui signifie que $\alpha\delta - \beta\gamma$ est plus grand que zéro.

Si, à partir de cette forme *réduite*, on continue le même mode de transformation, on obtient la *période* toujours composée d'un nombre limité de formes, au delà desquelles elle se reproduit.

Cela posé, on commence les transformations de $\left(D, N, \frac{N^2 - A}{D}\right)$ jusqu'à la *réduite*. On opère alors sur la proposée (a, b, c) jusqu'à la *réduite* d'abord; puis, en continuant, on forme sa période, jusqu'à ce qu'on rencontre, s'il est possible, la *réduite* de l'autre forme. Le but étant de trouver une forme commune aux deux suites, le travail s'abrégera de lui-même, si cette forme commune vient à se déclarer dans les deux suites, avant la formation de la période.

Il en résulte alors une série de formes qui commencent à (a, b, c), et se terminent à $\left(D, N, \frac{N^2 - A}{D}\right)$; mais, pour la réaliser, il faut avoir soin de supprimer la forme commune, et de prendre dans un ordre inverse, pour faire suite aux formes déduites de (a, b, c), les formes qui proviennent de $\left(D, N, \frac{N^2 - A}{D}\right)$. Il faut, de plus, dans chacune de ces dernières, remplacer le signe du terme moyen par un signe contraire, et faire changer de place entre eux aux termes extrêmes. C'est ce que Gauss appelle substituer à ces formes les *opposées* de leurs *associées*.

Toutes ces formes, dans leur enchaînement ainsi défini, ont, de l'une à l'autre, une relation constante que voici, c'est que le premier terme de chacune d'elles est égal au dernier terme de la forme précédente, et que la somme des deux termes moyens considérés dans deux formes consécutives, est exactement divisible par le terme qui leur est commun. Ces conditions, jointes à ce que, dans tous ces trinômes, $b^2 - ac = A$ (*), assurent ce que Gauss entend par leur *équivalence propre*, c'est-à-dire la propriété qu'elles ont de donner les représentations du nombre D, qui appartiennent à la valeur N de $\sqrt{A}$ (mod. D).

Voici, dès lors, l'*algorithme* particulier qui sert à déterminer les valeurs α, β, γ, δ dont on a besoin pour passer, directement, de la première forme à l'une quelconque de celles qui la suivent.

(*) Suivant la dénomination de Gauss, ces formes sont *contiguës*.

Représentons les formes trinomes successives par

$$(a, b, a'); \qquad (a', b', a''); \qquad (a'', b'', a'''); \ \ldots \text{ etc.};$$

et posons $\frac{b+b'}{a'} = h'$; $\frac{b'+b''}{a''} = h''$; $\frac{b''+b'''}{a'''} = h'''$; ... etc.;

on aura, pour déterminer les valeurs

$$\alpha', \beta', \gamma', \delta'; \qquad \alpha'', \beta'', \gamma'', \delta''; \qquad \alpha''', \beta''', \gamma''', \delta'''; \ \ldots \text{ etc.}$$

propres à faire passer directement de la première forme à celles qui la suivent, la loi de formation indiquée dans le tableau que voici :

$$\begin{array}{llll}
\alpha' = 0\,; & \beta' = -1\,; & \gamma' = 1\,; & \delta' = h'\,; \\
\alpha'' = \beta'\,; & \beta'' = h''\beta'\,; & \gamma'' = \delta'\,; & \delta'' = h''\delta' - 1\,; \\
\alpha''' = \beta''\,; & \beta''' = h'''\beta'' - \beta'\,; & \gamma''' = \delta''\,; & \delta''' = h'''\delta'' - \delta'\,; \\
\ldots\,; & \ldots\,; & \ldots\,; & \ldots\,; \\
\text{etc.}\,; & \text{etc.}\,; & \text{etc.}\,; & \text{etc.}
\end{array}$$

A l'aide de cet algorithme facile à saisir, on pourra former les valeurs α, β, γ, δ dont on a besoin pour passer, directement, de la forme (a, b, c) à la forme $\left(D, N, \frac{N^2 - A}{D}\right)$, et alors $x = \alpha$, $y = \gamma$ seront une solution de la proposée.

Il y en aura ainsi une pour chaque valeur de N, *positive* ou *négative*, dans les limites de $-\frac{D}{2}$ à $\frac{D}{2}$, toutes les fois que la *réduite* de $\left(D, N, \frac{N^2 - A}{D}\right)$ se trouvera dans la période de (a, b, c). Ces diverses solutions obtenues, on aura toutes celles qui en dépendent respectivement, à l'aide des formules

$$x = \alpha t - \gamma A u, \qquad y = \gamma t - \alpha u,$$

t et u étant des valeurs quelconques propres à résoudre $T^2 - AU^2 = 1$, lesquelles se déduisent les unes des autres, au moyen de la loi déjà plusieurs fois indiquée, pourvu qu'on connaisse un seul système de ces valeurs (*).

Lorsque le second terme manque dans l'équation à résoudre, il suffit de considérer les valeurs *positives* de N jusqu'à $\frac{D}{2}$. En effet, suivant les principes de Gauss, les formes *opposées* $\left(D, N, \frac{N^2 - A}{D}\right)$, $\left(D, -N, \frac{N^2 - A}{D}\right)$ sont *équivalentes proprement* et *improprement* puisque la proposée (a, o, c)

(*) Nous avons respecté, autant que possible, les notations dont se sont servis les auteurs.

est *ambiguë*. Le calcul conduirait donc à la même série, bien que par des routes différentes.

A ceux qui n'ont pas l'habitude de cette langue difficile, qui n'a guère été parlée que par celui qui l'a faite, il suffit de dire que, si les valeurs $x = \alpha x' + \beta y'$, $y = \gamma x' + \delta y'$, substituées dans la proposée (a, o, c), donnent naissance à la forme $\left(D, N, \frac{N^2 - A}{D}\right)$ quand on prend $\beta = \frac{N\alpha - c\gamma}{D}$, $\delta = \frac{N\gamma + a\alpha}{D}$, les mêmes valeurs font naître la forme $\left(D, -N, \frac{N^2 - A}{D}\right)$ lorsqu'on remplace N par $-N$ dans les expressions de β et de δ. La *réciproque* étant vraie, il y a nécessairement autant de transformations d'une espèce que de l'autre, de sorte qu'on trouvera les mêmes solutions pour la représentation de D, quel que soit celui des deux modes de calcul que l'on aura voulu suivre.

Telles sont les méthodes dont nous ne pouvons faire qu'un résumé rapide; le procédé que nous avons donné pour résoudre $x^2 - Ay^2 = r^m$, réussit toujours, dans le cas particulier de $A = a^2 + r$, si m est pair, et dans celui de $A = a^2 - r$, quel que soit m; et, lorsqu'il s'agit de l'équation $x^2 - Ay^2 = -r^m$, il réussit encore dans le cas de $A = a^2 + r$, pourvu que m soit impair.

Les solutions indépendantes de r et celles qui en dépendent, si faciles à découvrir par notre méthode, servent à déterminer toutes celles qui leur sont *semblables* avec le secours des formules déjà citées. Notre principe met donc en évidence, dans les cas particuliers que nous avons indiqués, la possibilité de résoudre les équations de la forme $x^2 - Ay^2 = \pm r^m$, et les diverses formes de solutions que l'on peut toujours obtenir, ce que les méthodes connues jusqu'ici n'établissent qu'après les calculs laborieux tentés pour leur résolution. Mais on peut se demander si, dans ces mêmes cas particuliers, les méthodes générales que nous avons essayé de reproduire, ne feraient pas découvrir plusieurs séries de solutions là où nous n'en trouvons qu'une, de sorte qu'il reste à faire voir qu'il n'en peut exister qu'une de chaque espèce. Nous ferons observer à cet égard que les méthodes de Gauss et de Legendre, pour trouver un carré N^2 égal à $A + Dt$, conduisent, dans l'hypothèse de $D = \pm r^m$, à une expression de la forme $N = r^m t + A$, et qu'ainsi, avec la condition imposée à N de

ne pas dépasser $\frac{r''}{2}$, il ne saurait exister qu'une valeur de N, et, partant, qu'une seule série de valeurs. Il est vrai que le premier cas traité par Legendre, celui de $D < \sqrt{A}$, échappe à ce raisonnement, puisque, dans cette hypothèse, il procède au développement de $\sqrt{A}$, sans aucune transformation préalable; mais Gauss n'établit pas cette distinction, et il est d'ailleurs évident que la méthode proposée par Legendre pour le cas de $D > \sqrt{A}$, bien que plus longue dans la pratique, n'en est pas moins applicable au premier cas de $D < \sqrt{A}$.

Application de la méthode de Lagrange aux équations qui ont servi d'exemples.

1° $x^2 - 29y^2 = 7^3$. On pose $x = ny - 343z$, n est un nombre qui ne peut excéder $\frac{343}{2}$, et assujetti à la condition de rendre $n^2 - 29$ divisible par 343. La valeur $n = 83$, que l'on trouve, donne la transformée $20y^2 - 166yz + 343z^2 = 1$. Pour résoudre celle-ci, il faut développer l'une des racines de $20y^2 - 166y + 343 = 0$, jusqu'à la première *réduite*, de rang pair, correspondant au quotient complet dont le dénominateur est 1. Si on développe la plus grande des deux racines, savoir $y = \frac{83 + \sqrt{29}}{20}$, la *réduite* cherchée est $\frac{137}{31}$, et donne par conséquent $z = 31$, $y = 137$, et, par suite, $x = 738$ (*).

Si maintenant on appelle Φ et Ψ les diverses solutions de $\Phi^2 - 29\Psi^2 = 1$, toutes les solutions *semblables* de la proposée seront données par les formules

$$x = 738\Phi \pm 29.137.\Psi, \qquad y = 738\Psi \pm 137\Phi.$$

Quant aux valeurs de Φ et de Ψ, le développement de $\sqrt{29}$ donne, pour la première *réduite* de rang pair, correspondant au quotient complet

(*) Si on développait l'autre racine $\frac{83 - \sqrt{29}}{20}$, on trouverait, pour première solution, $x = 2278$, $y = 423$, solution comprise dans les formules générales qui suivent, où il suffit de faire $\Phi = 9801$, $\Psi = 1820$.

$\frac{\sqrt{29}+5}{1}$ (*), le nombre fractionnaire $\frac{9081}{1820}$, dont les deux termes devront être substitués à φ et à ψ dans la formule $\Phi+\sqrt{29}\Psi=(\varphi+\sqrt{29}\psi)^m$ destinée à déterminer les quantités dont il s'agit.

2° $x^2-19y^2=3^4$. On pose $x=ny-81z$, et l'on trouve $n=10$, d'où

$$y^2-20yz+81z^2=1, \text{ ou } (y-10z)^2-19z^2=1.$$

Tout se réduit donc à résoudre $y'^2-19z^2=1$. Pour cela on développe $\sqrt{19}$, et l'on trouve $\frac{170}{39}$ pour la *réduite* qui correspond au premier quotient complet ayant 1 pour dénominateur, lequel est $\frac{\sqrt{19}+4}{1}$. Comme cette *réduite* est de rang pair, elle résout l'équation $\Phi^2-19\Psi^2=1$, et, par conséquent, $y'^2-19z^2=1$. On a donc $z=39$, $y'=170$, $y=560$, $x=2441$.

Pour obtenir maintenant toutes les solutions *semblables* de la proposée, on aura les formules

$$x=2441\Phi\pm19.560\Psi, \qquad y=2441\Psi\pm560\Phi,$$

en désignant par Φ et Ψ les solutions diverses de $\Phi^2-19\Psi^2=1$, solutions que l'on peut déduire du système $\varphi=170$, $\psi=39$, à l'aide de $\Phi+\sqrt{19}\Psi=(\varphi+\sqrt{19}\psi)^m$, en faisant varier m.

3° $x^2-31y^2=-216$. x et y, ne pouvant être impairs ni l'un ni l'autre, doivent être de la forme $2x'$, $2y'$. Il s'agit donc de résoudre $x'^2-31y'^2=-54$. En posant $x=ny-54z$, on trouve $n=25$, et, pour la transformée, $11y'^2-50y'z+54z^2=-1$. Si nous développons alors l'une des racines de $11y'^2-50y'+54=0$, la *réduite* qui correspond au premier quotient complet $\frac{\sqrt{31}+5}{1}$, est $\frac{25}{9}$; et, comme elle est de rang impair, et par conséquent moindre que la racine développée, on a, pour résoudre la transformée, $y'=25$ et $z=9$, d'où l'on déduit $x'=139$, et, par suite, $x=278$, $y=50$ pour résoudre la proposée.

Pour obtenir les autres solutions de même espèce, il faut résoudre $\Phi^2-31\Psi^2=1$. On trouve, en développant $\sqrt{31}$, pour la *réduite* qui

(*) La première réduite correspondant au quotient complet $\frac{\sqrt{29}+5}{1}$, est $\frac{70}{13}$; mais elle est de rang impair, et serait une solution de $x^2-29y^2=-1$.

correspond au premier quotient complet $\frac{\sqrt{31}+5}{1}$, la valeur $\frac{1520}{273}$. Or cette *réduite* est plus grande que $\sqrt{31}$; on a donc, pour premier système, $\varphi = 1520$, $\psi = 273$; et les autres s'obtiendront au moyen de la relation $\Phi + \sqrt{31}\Psi = (\varphi + \sqrt{31}\,\psi)^n$. Ainsi l'expression générale des solutions cherchées sera

$$x = 278\Phi \pm 31.50\Psi, \quad y = 278\Psi \pm 50\Phi.$$

Si l'on fait $\Phi = 1520$ et $\Psi = 273$, et qu'on change les signes, on trouve $x = 590$, $y = 106$.

Application de la méthode de Gauss aux mêmes équations.

1° $x^2 - 29y^2 = 7^3$. Gauss donne une méthode pour trouver un carré N^2 dont A soit *résidu* suivant le *module* p^m, mais avec la condition indispensable que A soit *résidu* de p, ce qui est ici l'hypothèse.

Cette méthode conduit à $N = 83$, de sorte que la transformée $\left(D, N, \frac{N^2 - A}{D}\right)$ est (343, 83, 20).

Cela posé, voici la suite du calcul :

Formes de $\left(D, N, \frac{N^2 - A}{D}\right)$ jusqu'à sa *réduite* : (343, 83, 20); (20, —3, —1); (—1, 5, 4).

Formes de $x^2 - 29y^2$ jusqu'à sa *réduite* : (1, 0, —29); (—29, 0, 1).

Période de (—29, 0, 1) jusqu'à la *réduite* (—1, 5, 4) :

(—29, 0, 1); (1, 5, —4); (—4, 3, 5); (5, 2, —5); (—5, 3, 4); (4, 5, —1); (—1, 5, 4).

Formes successives et continues de (1, 0, —29) à (343, 83, 20) :

(1, 0, —29); (—29, 0, 1); (1, 5, —4); (—4, 3, 5); (5, 2, —5); (—5, 3, 4); (4, 5, —1); (—1, 3, 20); (20 — 83, 343); (343, 83, 20).

Valeurs de	α,	β,	γ,	δ:
	0,	— 1,	1,	0;
	— 1,	— 5,	0,	— 1;
	— 5,	11,	— 1,	2;
	11,	16,	2,	3;
	16,	— 27,	3,	— 5;
	— 27,	— 70,	— 5,	— 13;
	— 70,	587,	— 13,	109;
	587,	— 2278,	109,	— 423;
	— 2278,	— 587,	— 423,	— 109.

On aura donc, en changeant le signe, $x = 2278$, $y = 423$; et toutes les solutions semblables s'obtiendraient par les formules

$$x = 2278t - 29.423u, \qquad y = 423t - 2278u,$$

dans lesquelles t et u sont une solution quelconque de $T^2 - 29U^2 = 1$. Si on prend $t = 9801$ et $u = 1820$, on trouve la solution $x = 738$, $y = 137$, obtenue par l'autre méthode.

2° $x^2 - 19y^2 = 3^4$. On trouve d'abord $N = 10$.

Formes de $\left(D, N, \frac{N^2 - A}{D}\right)$ jusqu'à sa *réduite* : $(81, 10, 1)$; $1, 4, -3)$; $(-3, 2, 5)$.

Formes de $x^2 - 19y^2 = 3^4$ jusqu'à sa *réduite* : $(1, 0, -19)$; $(-19, 0, 1)$;

Période de $(-19, 0, 1)$ jusqu'à la *réduite* $(-3, 2, 5)$:

$$(-19, 0, 1); \quad (1, 4, -3); \quad (-3, 2, 5).$$

L'apparition d'une forme commune aux deux suites, savoir $(1, 4, -3)$, avant la *réduite* $(-3, 2, 5)$, abrége un peu le travail.

Formes successives et continues de $(1, 0, -19)$ à $(81, 10, 1)$:

$$(1, 0, -19); \quad (-19, 0, 1); \quad (1, -10, 81); \quad (81, 10, 1).$$

Calcul des valeurs

α,	β,	γ,	δ :
0,	-1,	1,	0;
-1,	10,	0,	-1;
10,	1,	-1,	0;

d'où il résulte $x = 10$, $y = -1$.

Les valeurs *semblables* seront données par les formules générales

$$x = 10t - 19u, \qquad y = t - 10u;$$

et, si on prend $t = 170$, $u = -39$, valeurs qui résolvent $T^2 - 19U^2 = 1$, on trouve $x = 2441$, $y = 560$, solution déjà trouvée.

3° $x^2 - 31y^2 = -216$, ou plutôt $x'^2 - 31y'^2 = -54$, puisqu'il faut poser $x = 2x'$, $y = 2y'$. On trouve d'abord $N = 25$.

Formes de $\left(D, N, \frac{N^2 - A}{D}\right)$: $(-54, 25, -11)$; $(-11, -3, 2)$; $(2, 5, -3)$.

Formes de $(1, 0, -31)$ jusqu'à la forme $(2, 5, -3)$:

(1, 0, —31); (—31, 0, 1); (1, 5, —6); (—6, 1, 5); (5, 4, —3); (—3, 4, 2); (2, 5—3).

Formes continues de $x^2 - 31y^2$ jusqu'à la forme $\left(D, N, \frac{N^2 - A}{D}\right)$:

(1, 0, —31); (—31, 0, 1); (1, 5, —6); (—6, 1, 5); (5, 4, —3);
(—3, 5, 2); (2, 3, —11); (—11, —25, —54); (—54, 25, —11).

Calcul des valeurs

α,	β,	γ,	δ :
0,	— 1,	1,	0;
— 1,	— 5,	0,	— 1;
— 5,	6,	— 1,	1;
6,	11,	1,	2;
11,	— 39,	2,	— 7;
— 39,	— 167,	— 7,	— 30;
— 167,	— 295,	— 30,	— 53;
— 295,	167,	— 53,	30;

d'où l'on déduit $x' = 295$, $y' = 53$; et, par suite, $x = 590$, $y = 106$.

On aurait pour les valeurs *semblables*

$$x = 590t - 31.106u, \qquad y = 106t - 590u;$$

et, si on prend $t = 1520$, $u = 273$, valeurs qui résolvent $T^2 - AU^2 = 1$, on trouve la solution précédemment obtenue $x = 278$, $y = 50$.

Dans l'application des deux méthodes nous avons suivi, pour la détermination de n et de N, les procédés indiqués par les auteurs ; mais nous avons également obtenu leurs valeurs par un procédé particulier, que la longueur de ce mémoire, déjà trop étendu, nous empêche d'exposer ici.

FIN DES NOTES DU CINQUIÈME MÉMOIRE.

Paris. — Typographie de Firmin Didot frères, fils et Ce, rue Jacob, 56.

SIXIÈME MÉMOIRE

SUR

LA THÉORIE DES NOMBRES,

PAR M. F. LANDRY,

LICENCIÉ ÈS SCIENCES MATHÉMATIQUES.

Novembre 1856.

BODLEIANA BIBLIOTHECA

THÉORÈME DE FERMAT.

RECHERCHES NOUVELLES. — PREMIÈRE PARTIE. — TROISIÈME ET DERNIER LIVRE.

PARIS,

LIBRAIRIE DE L. HACHETTE ET Cie,

RUE PIERRE-SARRAZIN, N° 14,

(Près de l'École de médecine).

1856.

OUVRAGES DÉJA PUBLIÉS.

Premier mémoire, sur un Théorème de Legendre. Février 1853.

Second mémoire, Recherches nouvelles sur le théorème de Fermat. Premier livre. Juillet 1853.

Troisième mémoire, Nouvelle méthode pour la détermination des *racines primitives*. Mars 1854.

Table des nombres *premiers*, de 1 à 10000. Février 1855.

Tables des nombres entiers non divisibles par 2, 3, 5 et 7, jusqu'à 10201, avec leurs diviseurs simples en regard, et des carrés des 1000 premiers nombres. Février 1855.

Quatrième mémoire, deuxième livre des Recherches nouvelles sur le théorème de Fermat. Février 1855.

Cinquième mémoire, Théorème sur les réduites d'une nouvelle espèce de fractions *continues*. Juillet 1856.

THÉORÈME DE FERMAT,

RECHERCHES NOUVELLES. — PREMIÈRE PARTIE. — TROISIÈME ET DERNIER LIVRE.

Dans ce troisième livre, nous nous proposons d'appliquer les principes des deux livres précédents, et de démontrer que, relativement aux nombres *premiers* θ de la forme $2k\varphi n + 1$, les deux relations $1 + \varepsilon + \varepsilon^{\varepsilon} \equiv 0$, $1 + \varepsilon \equiv \varepsilon^{\varepsilon}$ sont impossibles pour $\varphi = 5$, $\varphi = 7$, $\varphi = 11$, $\varphi = 13$, $\varphi = 17$, et $\varphi = 19$. Trois exceptions nouvelles, seulement, devront être ajoutées au tableau, que nous avons donné dans le second livre, des facteurs θ qui échappent à notre analyse.

On ne doit pas oublier que n est un nombre *premier* plus grand que 2, et que ε est une racine de $x^{\varphi} \equiv 1$, autre que l'unité.

PREMIER PRINCIPE.

Les relations $1 + \varepsilon + \varepsilon^{\varepsilon} \equiv 0$, $1 + \varepsilon \equiv \varepsilon^{\varepsilon}$ sont impossibles pour $\varphi = 5$, et pour $\varphi = 7$.

L'impossibilité des deux relations proposées résulte immédiatement des principes généraux.

Ainsi, pour $\varphi = 5$, l'absurdité est démontrée par le premier principe du livre second, dans les cas de $z = 1$ et de $z = 5$; et par le deuxième, dans les cas de $z = 2$, $z = 3$, $z = 4$.

Pour $\varphi=7$, l'absurdité est établie par le premier principe du même livre, dans les cas de $z=1$ et de $z=7$; par le second, dans les cas de $z=2$, $z=4$, $z=6$; et par les troisième et quatrième, dans les cas de $z=3$ et de $z=5$.

Pour ces deux valeurs de φ, il n'y a pas d'exception au delà de $n=3$.

DEUXIÈME PRINCIPE.

Les relations $1+\varepsilon+\varepsilon^z\equiv 0$, $1+\varepsilon\equiv\varepsilon^z$ sont impossibles pour $\varphi=11$.

Le premier principe du second livre met en évidence l'impossibilité des proposées dans le cas de $z=1$, et dans celui de $z=11$.

Le second principe la démontre pour $z=2$, $z=6$, $z=10$.

Enfin, le troisième et le quatrième la rendent incontestable pour $z=3$, $z=4$, $z=5$, $z=7$, $z=8$, et $z=9$ (*).

La proposition n'admet, au delà de $n=3$, qu'une seule exception, celle indiquée au tableau du second livre pour $\varphi=11$, savoir $\theta=683$ dans le cas de $n=31$.

TROISIÈME PRINCIPE.

Les deux relations $1+\varepsilon+\varepsilon^z\equiv 0$, $1+\varepsilon\equiv\varepsilon^z$ sont impossibles pour $\varphi=13$.

L'impossibilité résulte des deux premiers principes du second livre, pour les valeurs $z=1$, $z=2$, $z=7$, $z=12$, et $z=13$.

(*) Voyez la première note, page 16

Elle résulte des troisième et quatrième principes, pour $z=3$, $z=5$, $z=6$, $z=8$, $z=9$, et $z=11$ (*).

Il reste donc à examiner l'impossibilité des deux relations pour l'une des deux valeurs $z=4$, $z=10$; car ces deux cas se réduisent à un seul, d'après le deuxième principe du premier livre.

Commençons par démontrer l'impossibilité de $1+\varepsilon+\varepsilon^4\equiv 0$.

En carrant $1+\varepsilon^4\equiv-\varepsilon$, on trouve la relation $1+2\varepsilon^4+\varepsilon^8\equiv\varepsilon^2$. Mais, si l'on donne à la proposée la forme $\varepsilon^{10}+\varepsilon^{11}\equiv-\varepsilon$, et que l'on carre, on trouve $\varepsilon^7+2\varepsilon^8+\varepsilon^9\equiv\varepsilon^2$: on a donc $1+2\varepsilon^4+\varepsilon^8\equiv\varepsilon^7+2\varepsilon^8+\varepsilon^9$ où $1+2\varepsilon^4\equiv\varepsilon^7+\varepsilon^8+\varepsilon^9$, d'où l'on déduit successivement $1+2\varepsilon^4+\varepsilon^{12}\equiv\varepsilon^7$, $2\varepsilon^4\equiv\varepsilon^7+\varepsilon^3$, et $3\equiv 0$.

Reste le seul cas de $1+\varepsilon\equiv\varepsilon^4$.

Formons la septième puissance de cette relation, et réduisons: nous trouvons $\varepsilon^{12}+\varepsilon^8+\varepsilon^4+1+\varepsilon^9+\varepsilon^4+\varepsilon\equiv 0$ (**), et, par suite, $3\varepsilon^4+2\varepsilon^{12}\equiv 0$, à cause de $\varepsilon^8+\varepsilon^9\equiv\varepsilon^{12}$. Le dernier résultat obtenu conduit à la condition numérique $3^{13}\equiv-2^{13}$ ou $1602515\equiv 0$. Or ce nombre, qui est égal à $5.79.4057$, ne saurait être un multiple de $2k\varphi n+1$, pour $\varphi=13$, n étant plus grand que 3, si ce n'est dans le cas de 4057, pour $n=13$. On a en effet $79=2.3.13+1$, et $4057=2.2.2.3.13.13+1$. Pour faire disparaître cette exception, cherchons d'autres conditions numériques.

1° Formons les diverses puissances de $3\varepsilon^4+2\varepsilon^{12}\equiv 0$ ou plutôt de $3\varepsilon^5\equiv-2$; et cherchons, dans les relations nouvelles, celles qui contiennent les exposants de ε considérés dans l'une des trois formes $1+\varepsilon\equiv\varepsilon^4$, $\varepsilon^{12}+1\equiv\varepsilon^3$, $\varepsilon^9+\varepsilon^{10}\equiv 1$, de la proposée. Nous aurons ainsi les éléments d'une élimination facile. Voici ces relations :

$3\varepsilon^5\equiv-2$ ou $2\varepsilon^8\equiv-3$; $9\varepsilon^{10}\equiv 4$ ou $4\varepsilon^3\equiv 9$; $27\varepsilon^2\equiv-8$ ou $8\varepsilon^{11}\equiv-27$; $81\varepsilon^7\equiv 16$ ou $16\varepsilon^6\equiv 81$; $243\varepsilon^{12}\equiv-32$ ou $32\varepsilon\equiv-243$.

Prenons $4\varepsilon^3\equiv 9$ et $243\varepsilon^{12}\equiv-32$ pour éliminer avec $\varepsilon^{12}+1\equiv\varepsilon^3$: nous trouverons $1343\equiv 0$. Or ce dernier nombre, qui est égal à 17.79,

---

(*) Voyez la seconde note, page 18.

(**) Voyez, pour ce développement, la note troisième, page 21.

ne saurait être un multiple de $2h\varphi n + 1$ pour $\varphi = 13$, si on suppose n plus grand que 3.

2° Voici encore une élimination assez rapide :

Les deux relations $3\varepsilon^4 + 2\varepsilon^{12} \equiv 0$, $1 + \varepsilon \equiv \varepsilon^4$ conduisent à $2\varepsilon^{12} + 3\varepsilon \equiv -3$, d'où l'on déduit, en carrant deux fois de suite, $4\varepsilon^{11} + 9\varepsilon^2 \equiv -3$, $16\varepsilon^9 + 81\varepsilon^4 \equiv -63$. Mais, $3\varepsilon^4 + 2\varepsilon^{12} \equiv 0$ pouvant être mis sous la forme $3\varepsilon^9 + 2\varepsilon^4 \equiv 0$, il devient facile d'éliminer, et l'on trouve $68335 \equiv 0$. Or ce dernier nombre est égal à $5.79.173$, et $173 = 2.2.43 + 1$.

Les deux résultats que nous venons d'obtenir, conduisent donc, comme celui qui avait précédé, à la même condition numérique $79 \equiv 0$, et servent à écarter l'exception du facteur 4057. En conséquence il n'y aurait d'objection nouvelle à l'impossibilité de $1 + \varepsilon \equiv \varepsilon^4$ que pour le seul facteur 79, dans les cas de $n = 1$ et de $n = 3$.

On voit, en définitive, que, pour ce troisième principe, il n'y a aucune exception à ajouter à celles qui ont été indiquées, au tableau du second livre, pour $\varphi = 13$.

QUATRIÈME PRINCIPE.

Les relations $1 + \varepsilon + \varepsilon^z \equiv 0$, $1 + \varepsilon \equiv \varepsilon^z$, sont impossibles pour $\varphi = 17$.

Les quatre principes du second livre démontrent l'impossibilité des deux relations, le premier pour $z = 1$ et $z = 17$; le second pour $z = 2$, $z = 9$, $z = 16$; le troisième et le quatrième pour $z = 3$, $z = 6$, $z = 8$, $z = 10$, $z = 12$, et $z = 15$.

En conséquence les seuls cas restant à examiner, dans les deux relations, sont ceux de $z = 4$, $z = 5$, $z = 7$, $z = 11$, $z = 13$, $z = 14$.

L'examen de ces valeurs dans la première relation, se réduit à un seul cas, eu égard au troisième principe du premier livre.

Quant à leur examen dans la seconde relation, on peut choisir ou d'es-

sayer, en raison du deuxième principe du premier livre, l'une des valeurs de chacun des trois groupes binaires 4,14; 5,13; 7,11; ou bien d'essayer, conformément au quatrième principe du même livre, une seule de ces six valeurs dans les trois relations

$$1+\varepsilon-\varepsilon^z\equiv 0,\qquad 1-\varepsilon+\varepsilon^z\equiv 0,\qquad -1+\varepsilon+\varepsilon^z\equiv 0.$$

Nous ferons usage du premier mode d'examen (*).

Commençons par démontrer l'impossibilité de la relation $1+\varepsilon+\varepsilon^z\equiv 0$ pour $z=4$.

On trouve, en multipliant $1+\varepsilon+\varepsilon^4\equiv 0$ par $1+\varepsilon^3+\varepsilon^5+\varepsilon^{10}+\varepsilon^{15}$, puis ajoutant de part et d'autre $\varepsilon^8+\varepsilon^{12}+\varepsilon^{13}$, et réduisant : $\varepsilon^4\equiv\varepsilon^8+\varepsilon^{12}+\varepsilon^{13}$. Ce résultat devient successivement $\varepsilon^4+\varepsilon^{16}\equiv\varepsilon^8$, $1+\varepsilon^{12}\equiv\varepsilon^4$, et enfin $1+\varepsilon'\equiv\varepsilon'^6$, si on pose $\varepsilon^{12}\equiv\varepsilon'$ d'où $\varepsilon\equiv\varepsilon'^{10}$, $\varepsilon^4\equiv\varepsilon'^6$. Or l'absurdité de $1+\varepsilon\equiv\varepsilon^z$ est démontrée pour $z=6$.

Occupons-nous maintenant de l'impossibilité de la relation $1+\varepsilon\equiv\varepsilon$ pour $z=4$, $z=5$, et $z=7$.

Première hypothèse $z=4$.

Si on développe la cinquième puissance de $1+\varepsilon\equiv\varepsilon^4$, et qu'on réduise, on trouve $3\varepsilon^{13}+\varepsilon^4\equiv-2\varepsilon^8$ (**). Cette relation rentre dans la forme générale $a\varepsilon^n+b\varepsilon^{-n}\equiv c\varepsilon^{2n}$, mais la méthode conduit à des nombres considérables qu'il importe d'éviter. Or, à cause de $\varepsilon^8\equiv\varepsilon^4+\varepsilon^5$, la relation $3\varepsilon^{13}+\varepsilon^4\equiv-2\varepsilon^8$ devient $3\varepsilon^{13}+3\varepsilon^4+2\varepsilon^5\equiv 0$, et peut prendre l'une des formes $3\varepsilon^8+2\varepsilon^9\equiv-3$, $3\varepsilon^{16}+2\equiv-3\varepsilon^8$. Ces derniers résultats peuvent servir à l'élimination de ε, avec $9\varepsilon^9+\varepsilon^8\equiv 4\varepsilon^{16}-6$ obtenu par l'élévation de $3\varepsilon^{13}+\varepsilon^4\equiv-2\varepsilon^8$ au carré. Faisant d'abord disparaître ε^{16}, on a $27\varepsilon^9+15\varepsilon^8\equiv-26$; puis éliminant successivement avec $3\varepsilon^8+2\varepsilon^9\equiv-3$, les deux puissances ε^8 et ε^9, on trouve les deux résultats $17\varepsilon^9\equiv-11$, $51\varepsilon^8\equiv-29$, qui, multipliés membre à membre, donnent $548\equiv 0$. Or $548=2.2.137$, et $137=2.2.2.17+1$: il n'y a donc pas d'exception pour n plus grand que 2.

(*) Voyez la note quatrième, page 21, sur l'emploi du second mode d'examen.

(**) Voyez, pour le développement, la note cinquième, à la page 22.

Deuxième hypothèse $z = 5$.

Si on cube la relation $1 + \varepsilon \equiv \varepsilon^5$, on trouve $1 + 3\varepsilon^6 + \varepsilon^3 \equiv \varepsilon^{15}$; mais de $1 + \varepsilon \equiv \varepsilon^5$ on tire $\varepsilon^{15} + \varepsilon^{16} \equiv \varepsilon^3$: donc, en ajoutant, on aura $1 + 3\varepsilon^6 + \varepsilon^{16} \equiv 0$, et, par suite, $3\varepsilon^6 + \varepsilon^4 \equiv 0$, d'où l'on conclura $3^{17} \equiv -1$.

Pour éviter d'avoir à considérer la dix-septième puissance de 3, on déduit, de $3\varepsilon^6 + \varepsilon^4 \equiv 0$, la relation $3\varepsilon^2 \equiv -1$, d'où $9\varepsilon^4 \equiv 1$; et, après avoir mis $1 + \varepsilon \equiv \varepsilon^5$ sous la forme $\varepsilon^{16} + 1 \equiv \varepsilon^4$, on obtient, par l'élimination de ε^4 : $9\varepsilon^{16} \equiv -8$ ou $9 \equiv -8\varepsilon$, ce qui donne enfin $64\varepsilon^2 \equiv 81$. Cette dernière relation, combinée avec $3\varepsilon^2 \equiv -1$, conduit à $307 \equiv 0$ ou $2.3.3.17 + 1 \equiv 0$.

On peut obtenir la même condition numérique, comme il suit. Les formes de la proposée étant $1 + \varepsilon \equiv \varepsilon^5$, $\varepsilon^{12} + \varepsilon^{13} \equiv 1$, $\varepsilon^{16} + 1 \equiv \varepsilon^4$, il s'agit de déduire de $3\varepsilon^2 \equiv -1$ les deux puissances de ε nécessaires à l'élimination. Or la série est :

$3\varepsilon^2 \equiv -1$ ou $\varepsilon^{15} \equiv -3$; $9\varepsilon^4 \equiv 1$ ou $\varepsilon^{13} \equiv 9$; $27\varepsilon^6 \equiv -1$ ou $\varepsilon^{11} \equiv -27$; $81\varepsilon^8 \equiv 1$ ou $\varepsilon^9 \equiv 81$; $243\varepsilon^{10} \equiv -1$ ou $\varepsilon^7 \equiv -243$; $729\varepsilon^{12} \equiv 1$ ou $\varepsilon^5 \equiv 729$.

On obtient donc facilement, en combinant les trois relations $\varepsilon^{12} + \varepsilon^{13} \equiv 1$, $\varepsilon^{13} \equiv 9$, $729\varepsilon^{12} \equiv 1$, la condition $5833 \equiv 0$ ou $19.307 \equiv 0$: ainsi il n'y a pas d'exception au-delà de $n = 3$.

Troisième hypothèse $z = 7$.

Si on forme la cinquième puissance de $1 + \varepsilon \equiv \varepsilon^7$, et qu'on réduise, on trouve $3\varepsilon^5 + \varepsilon^8 + 2 \equiv 0$ (*) ou $3\varepsilon^7 + \varepsilon^{10} \equiv -2\varepsilon^2$. Or, en carrant $1 - \varepsilon^7 \equiv -\varepsilon$, on trouve $1 + \varepsilon^{14} - 2\varepsilon^7 \equiv \varepsilon^2$: donc $3\varepsilon^7 + \varepsilon^{10} \equiv -2 - 2\varepsilon^{14} + 4\varepsilon^7$ ou $\varepsilon^7 - \varepsilon^{10} \equiv 2\varepsilon^{14} + 2$, résultat que l'on peut mettre sous la forme $2\varepsilon^{10} + 2\varepsilon^7 \equiv 1 - \varepsilon^3$ (**).

Élevons au carré la première de ces deux dernières relations, nous trouvons $\varepsilon^3 - 7\varepsilon^{14} \equiv 4\varepsilon^{11} + 6$; et, si on élimine alors ε^3 et ε^{14}, on ob-

---

(*) Voyez, pour ce développement, la note sixième, page 23.

(**) On pourrait appliquer la méthode générale à ces deux relations, mais on serait conduit à de très-grands nombres.

tient $3\varepsilon^{10} - 11\varepsilon^7 \equiv 8\varepsilon^{11} - 4$, qui, à cause de $8\varepsilon^{10} + 8\varepsilon^{11} \equiv 8$, prend la forme $11\varepsilon^{10} - 11\varepsilon^7 \equiv 4$. On obtient alors très-simplement $11\varepsilon^{14} \equiv -13$ ou $13\varepsilon^3 \equiv -11$, et, par suite, $13\varepsilon^{10} + 13\varepsilon^7 \equiv 12$ d'où il est facile de déduire successivement $143\varepsilon^{10} \equiv 92$, $143\varepsilon^7 \equiv 40$, et $16769 \equiv 0$. Or 16769, qui est égal à 41.409, ne saurait être un multiple de $2k\varphi n + 1$ pour $\varphi = 17$, si ce n'est pour $\theta = 409$ dans les cas de $n = 1$, $n = 2$, et de $n = 3$, à cause de $409 = 2.2.2.3.17 + 1$. Si on comparait $13\varepsilon^{10} + 13\varepsilon^7 \equiv 12$ avec $11\varepsilon^{10} - 11\varepsilon^7 \equiv 4$ mis sous la forme $33\varepsilon^{10} - 33\varepsilon^7 \equiv 12$, on obtiendrait $10\varepsilon^3 \equiv 23$ qui, combiné avec $11\varepsilon^{14} \equiv -13$, donnerait $409 \equiv 0$.

Ainsi le quatrième principe ne peut comporter pour θ, n étant plus grand que 3, d'autres exceptions que celles qui ont été indiquées au tableau du second livre pour $\varphi = 17$.

CINQUIÈME PRINCIPE.

Les relations $1 + \varepsilon + \varepsilon^z \equiv 0$, $1 + \varepsilon \equiv \varepsilon^z$ sont impossibles pour $\varphi = 19$.

L'impossibilité est démontrée par les quatre principes du second livre, savoir :

Par le premier,

pour $z = 1$ et $z = 19$;

Par le second,

pour $z = 2$, $z = 10$, et $z = 18$;

Par les deux derniers,

pour $z = 3$, $z = 7$, $z = 9$, $z = 11$, $z = 13$ et $z = 17$.

Il reste donc à démontrer l'impossibilité des deux relations dans les cas de $z = 4$, $z = 5$, $z = 6$, $z = 14$, $z = 15$, $z = 16$; et dans ceux de $z = 8$, $z = 12$.

Occupons-nous d'abord de l'impossibilité de la relation $1 + \varepsilon + \varepsilon^z \equiv 0$. D'après le troisième principe du premier livre, il suffira de considérer le cas de $z = 4$ pour les six premières valeurs de z, et celui de $z = 8$ pour les deux autres.

Première hypothèse $z=4$.

Multipliez la relation $1+\varepsilon+\varepsilon^4\equiv 0$ par $1+\varepsilon^2+\varepsilon^7+\varepsilon^9+\varepsilon^{14}+\varepsilon^{16}$, ajoutez de part et d'autre $\varepsilon^5+\varepsilon^{12}$, et réduisez, vous trouverez $\varepsilon\equiv\varepsilon^5+\varepsilon^{12}$ ou $1+\varepsilon^7\equiv\varepsilon^{15}$; et, en posant $\varepsilon^7\equiv\acute{\varepsilon}$, d'où $\varepsilon\equiv\varepsilon'^{11}$, on aura $1+\varepsilon'\equiv\varepsilon'^{13}$ relation qui rentre dans celles dont l'impossibilité est démontrée.

Deuxième hypothèse $z=8$.

Multiplions $1+\varepsilon+\varepsilon^8\equiv 0$ par $1+\varepsilon^3+\varepsilon^4+\varepsilon^9+\varepsilon^{13}+\varepsilon^{15}+\varepsilon^{17}$, ajoutons ε^7 de part et d'autre, et réduisons : nous trouvons $2\varepsilon^4+\varepsilon^{17}\equiv\varepsilon^7$ ou $2\varepsilon^3+\varepsilon^{16}\equiv\varepsilon^6$ relation à laquelle peut s'appliquer la méthode des séries. Pour les éviter, on a d'abord $2+\varepsilon^{13}\equiv\varepsilon^3$; mais de $1+\varepsilon^8\equiv-\varepsilon$ on obtient $1+\varepsilon^{16}+2\varepsilon^8\equiv\varepsilon^2$ qui, par l'élimination de ε^2 avec $2\varepsilon^8+\varepsilon^2\equiv\varepsilon^{11}$, donne $\varepsilon^{11}-4\varepsilon^8\equiv\varepsilon^{16}+1$ dont le carré est $\varepsilon^3+14\varepsilon^{16}\equiv\varepsilon^{13}+9$. Ces deux dernières relations sont également abordables par les séries, mais on peut éliminer immédiatement ε^3 et ε^{13}, si on ajoute membre à membre $2+\varepsilon^{13}\equiv\varepsilon^3$ avec $\varepsilon^3+14\varepsilon^{16}\equiv\varepsilon^{13}+9$: on trouve, en effet, $2\varepsilon^{16}\equiv 1$; et, comme on en déduit, en carrant, $4\varepsilon^{13}\equiv 1$, on peut éliminer ε^{13}. On arrive ainsi à $4\varepsilon^3\equiv 9$, et enfin à $8\equiv 9$ ou $1\equiv 0$, en multipliant membre à membre cette dernière condition avec $2\varepsilon^{16}\equiv 1$.

Occupons-nous maintenant de l'impossibilité de la relation $1+\varepsilon\equiv\varepsilon^z$ pour les valeurs $z=4$, $z=5$, $z=6$, $z=14$, $z=15$, $z=16$; $z=8$, et $z=12$.

D'après le deuxième principe du premier livre, l'examen de ces diverses hypothèses se réduit à celui des valeurs $z=4$, $z=5$, $z=6$, $z=8$.

Première hypothèse $z=4$.

Formons la sixième puissance de $1+\varepsilon\equiv\varepsilon^4$: nous trouvons $5\varepsilon^{10}+5\varepsilon^5+\varepsilon^2+1\equiv 0$ (*). On déduit de cette dernière relation, $5\varepsilon^{12}+5\varepsilon^7\equiv-\varepsilon^4-\varepsilon^2$, $5\varepsilon^{12}+5\varepsilon^7\equiv-1-\varepsilon-\varepsilon^2$, $5\varepsilon^{12}+5\varepsilon^7\equiv-1-\varepsilon^5$

(*) Voyez, pour le développement, la note septième, page 23.

ou $\varepsilon^{12} + \varepsilon^7 \equiv -5 - 5\varepsilon^{14}$. Multipliant ce dernier résultat par 5, pour éliminer le premier membre, on trouve $25\varepsilon^{14} + 24 - \varepsilon^5 \equiv 0$.

Pour éviter les nombres considérables auxquels on serait conduit en appliquant les méthodes à la relation que nous venons d'obtenir, reprenons $5\varepsilon^{10} + 5\varepsilon^5 + \varepsilon^2 + 1 \equiv 0$. On trouve successivement $5\varepsilon^{11} + \varepsilon^8 \equiv -5\varepsilon^{16} - \varepsilon^6$, $25\varepsilon^3 + \varepsilon^{16} \equiv 25\varepsilon^{13} + \varepsilon^{12} + 10\varepsilon^3 - 10$, $15\varepsilon^3 \equiv 24\varepsilon^{13} - 10$, et $15\varepsilon^6 \equiv 24\varepsilon^{16} - 10\varepsilon^3$ qui se prêterait à la méthode.

Mais, sous la forme $10\varepsilon^{10} + 15\varepsilon^{13} \equiv 24\varepsilon^4$, la même relation devient $25\varepsilon^{10} + 15\varepsilon^9 \equiv 24\varepsilon^4$ à cause de $\varepsilon^{13} \equiv \varepsilon^9 + \varepsilon^{10}$. On pourra donc combiner cette dernière relation avec $25\varepsilon^{14} - \varepsilon^5 \equiv -24$ qui donne, au carré, $625\varepsilon^9 + \varepsilon^{10} \equiv 626$ ou $625 + \varepsilon \equiv 626\varepsilon^{10}$, et $624 + \varepsilon^4 \equiv 626\varepsilon^{10}$. L'élimination de ε^4 donne $14976 + 15\varepsilon^9 \equiv 14999\varepsilon^{10}$. Si maintenant nous éliminons successivement ε^9 puis ε^{10}, nous trouvons $937439\varepsilon^{10} \equiv 936939$, $4687195\varepsilon^9 \equiv 4687199$, et $23398749744 \equiv 0$. Ce dernier nombre est égal à $2.2.2.2.761.192169$. Mais, pour éviter d'avoir à vérifier si 192169 est un nombre *premier;* cherchons une autre relation.

De $25\varepsilon^{14} - \varepsilon^5 \equiv -24$, on déduit successivement $25\varepsilon^9 - 1 \equiv -24\varepsilon^{14}$, $25\varepsilon^5 + 25\varepsilon^6 - 1 \equiv -24\varepsilon^{14}$, $625\varepsilon^5 + 625\varepsilon^6 - 25 \equiv -24\varepsilon^5 + 576$, $649\varepsilon^5 + 625\varepsilon^6 \equiv 601$, $649\varepsilon^9 + 625\varepsilon^{10} \equiv 601\varepsilon^4$. Mais on a trouvé $25\varepsilon^{10} + 15\varepsilon^9 \equiv 24\varepsilon^4$: l'élimination de ε^4 donnera donc $65611\varepsilon^9 - 25\varepsilon^{10} \equiv 0$; et, comme en carrant $25\varepsilon^{14} - \varepsilon^5 \equiv -24$, on a déjà obtenu $625\varepsilon^9 + \varepsilon^{10} \equiv 626$, on arrive aux résultats successifs $15625\varepsilon^9 + 25\varepsilon^{10} \equiv 15650$, $22186\varepsilon^9 \equiv 15650$ ou $11093\varepsilon^9 \equiv 7825$, $11093\varepsilon^{10} \equiv 2053593$, et $15946310576 \equiv 0$. Or $15946310576 \equiv 2.2.2.2.7.761.187093$, et 187093 est *premier* avec 192169. Ainsi il est clair qu'on ne saurait satisfaire aux deux conditions numériques précédentes, pour aucun facteur *premier* $2k\varphi n + 1$, si ce n'est pour le facteur $\theta = 761$; et, comme $761 = 2.2.2.5.19 + 1$, cela ne serait possible pour n plus grand que 2, que dans un seul cas, celui de $n = 5$.

Deuxième hypothèse $z = 5$.

Développons la quatrième puissance de $1 + \varepsilon \equiv \varepsilon^5$: nous trouvons successivement $\varepsilon^4 + 4\varepsilon^3 + 6\varepsilon^2 + 3\varepsilon + 1 \equiv 0$, $\varepsilon^8 + 3\varepsilon^7 + 3\varepsilon^6 + 1 \equiv 0$,

$3\varepsilon^{11} + \varepsilon^{8} + 1 \equiv 0$. Cette dernière relation est de la forme $a\varepsilon^{n} + \varepsilon^{-n} \equiv e$; et, si l'on forme la série des puissances impaires, à l'aide de *l'échelle de relation*, $9\varepsilon^{3} + \varepsilon^{16} \equiv -5$, et -9, les seconds membres des puissances

1, 3, 5, 7, 9, 11, 13, 15, 17, et 19,

seront

-1, 8, -31, 83, -136, -67, 1559, -7192, 21929, et -44917.

En conséquence il vient $3^{19} + 1 \equiv -44917$ ou $1162261467 + 1 \equiv -44917$ d'où il résulte $1162306385 \equiv 0$. Ce dernier nombre est égal à $5.647.359291$; et, pour ne pas avoir à nous occuper du troisième facteur, nous chercherons une autre relation.

De $3\varepsilon^{11} + \varepsilon^{8} \equiv -1$ élevé au cube, on déduit $27\varepsilon^{14} + \varepsilon^{5} \equiv 8$ ou $27 + \varepsilon^{10} \equiv 8\varepsilon^{5}$, $27 + \varepsilon^{10} \equiv 8 + 8\varepsilon$ ou $\varepsilon^{10} - 8\varepsilon \equiv -19$, et par conséquent $19\varepsilon^{9} - 8\varepsilon^{10} \equiv -1$. Mais le carré de $27\varepsilon^{14} + \varepsilon^{5} \equiv 8$ est $729\varepsilon^{9} + \varepsilon^{10} \equiv 10$: il reste donc à éliminer ε^{10} puis ε^{9}, ce qui donne $5851\varepsilon^{9} \equiv 79$, $5851\varepsilon^{10} \equiv 919$, et $34161600 \equiv 0$. Ce dernier nombre est égal à $2.2.2.2.2.2.3.5.5.11.647$; et, comme $647 = 2.17.19 + 1$, il est évident que, n ne pouvant être égal à 1, la condition est absurde, excepté pour le seul facteur 647 dans le cas de $n = 17$ et de $k = 1$.

Troisième hypothèse $z = 6$.

La relation $1 + \varepsilon \equiv \varepsilon^{6}$ donne, au cube, $\varepsilon^{3} + 3\varepsilon^{2} + 3\varepsilon + 1 \equiv \varepsilon^{18}$. On en déduit $\varepsilon^{4} + 3\varepsilon^{3} + 3\varepsilon^{2} + \varepsilon \equiv 1$, $\varepsilon^{4} + 3\varepsilon^{8} \equiv 1 - \varepsilon$, puis, en carrant, $\varepsilon^{8} + 9\varepsilon^{16} + 6\varepsilon^{12} \equiv (1 + \varepsilon)^{2} - 4\varepsilon$, $\varepsilon^{8} + 9\varepsilon^{16} + 5\varepsilon^{12} \equiv -4\varepsilon$, $5\varepsilon^{15} + 4\varepsilon^{4} \equiv -\varepsilon^{11} - 9$.

Cette relation peut donner une série, mais elle conduit rapidement à des nombres considérables. Il faut donc trouver une seconde relation qui puisse se combiner avec celle-là. Or, si on carre deux fois de suite $\varepsilon^{9} + \varepsilon^{16} \equiv \varepsilon^{15}$, on trouve successivement $\varepsilon^{18} + \varepsilon \equiv \varepsilon^{11} - 2$, $\varepsilon^{17} + \varepsilon^{2} \equiv \varepsilon^{3} + 2 - 4\varepsilon^{11}$. Mais on a $\varepsilon^{3} \equiv \varepsilon^{17} + \varepsilon^{16}$, $\varepsilon^{15} + \varepsilon^{16} \equiv \varepsilon^{2}$: donc, en ajoutant membre à membre ces trois dernières relations, on obtiendra $\varepsilon^{15} \equiv 2 - 4\varepsilon^{11}$, c'est-à-dire $2\varepsilon^{4} - 4\varepsilon^{15} \equiv 1$.

Ce résultat suffirait pour conduire au but, mais on évitera des nombres considérables, en le combinant avec $4\varepsilon^4 + 5\varepsilon^{15} \equiv -\varepsilon^{11} - 9$. En effet l'élimination de ε^4 donne $13\varepsilon^{15} \equiv -\varepsilon^{11} - 11$ ou $\varepsilon^{15} + 11\varepsilon^4 \equiv -13$. En continuant le calcul d'élimination, on arrive successivement à $46\varepsilon^4 \equiv -51$, $46\varepsilon^{15} \equiv -37$, et, par suite, à $229 = 0$, résultat absurde, dans l'hypothèse de $\varphi = 19$, excepté pour $\theta = 229$ dans les cas de $n = 1$, $n = 2$, $n = 3$, puisque 229, qui est *premier*, est égal à $2.2.3.19 + 1$. Ce facteur θ fait déjà partie de ceux qui échappent à notre analyse, pour les mêmes valeurs de φ, de n et de k.

Quatrième et dernière hypothèse $z = 8$.

Formons la cinquième puissance de $1 + \varepsilon \equiv \varepsilon^8$: nous trouvons, après avoir réduit, $3\varepsilon^6 + 2\varepsilon^8 \equiv 0$ (*). Cette relation suffirait, puisqu'elle donne immédiatement la condition numérique $3^{19} \equiv -2^{19}$, et par conséquent $1162785755 \equiv 0$ ou $232557151 \equiv 0$, après la suppression du facteur 5. Mais ce dernier nombre est égal à 419.555029; et, pour éviter l'appréciation du second facteur, nous allons chercher à éliminer, avec l'une des trois formes de la proposée,

$$1 + \varepsilon \equiv \varepsilon^8, \quad \varepsilon^{18} + 1 \equiv \varepsilon^7, \quad \varepsilon^{11} + \varepsilon^{12} \equiv 1,$$

en formant, à l'aide de $3\varepsilon^6 + 2\varepsilon^8 \equiv 0$, les puissances de ε nécessaires à cette élimination. On a, pour ces puissances,

$$\begin{array}{llllllll}
2\varepsilon^2 & \equiv -3 & \text{ou} & 3\varepsilon^{17} \equiv -2; & 4\varepsilon^4 & \equiv 9 & \text{ou} & 9\varepsilon^{15} \equiv 4; \\
8\varepsilon^6 & \equiv -27 & \text{ou} & 27\varepsilon^{13} \equiv -8; & 16\varepsilon^8 & \equiv 81 & \text{ou} & 81\varepsilon^{11} \equiv 16; \\
32\varepsilon^{10} & \equiv -243 & \text{ou} & 243\varepsilon^9 \equiv -32; & 64\varepsilon^{12} & \equiv 729 & \text{ou} & 729\varepsilon^7 \equiv 64.
\end{array}$$

On peut alors, pour éliminer, prendre les trois relations

$$81\varepsilon^{11} \equiv 16, \qquad 64\varepsilon^{12} \equiv 729, \qquad \varepsilon^{11} + \varepsilon^{12} \equiv 1,$$

lesquelles conduisent facilement à $54889 \equiv 0$. Or $54889 = 131.419$.

On peut arriver plus promptement encore. Prenons, en effet, dans la série précédente, le terme $16\varepsilon^8 \equiv 81$ pour éliminer avec $1 + \varepsilon \equiv \varepsilon^8$: nous trouvons $16 + 16\varepsilon \equiv 81$ ou $16\varepsilon \equiv 65$, et $16\varepsilon^2 \equiv 65\varepsilon$ résultat d'où l'on peut faire disparaître ε^2, à l'aide de $2\varepsilon^2 \equiv -3$ ou $16\varepsilon^2 \equiv -24$. On

(*) Voyez, pour le développement, la note huitième, page 24.

obtient alors $65\varepsilon \equiv -24$ qui, combiné avec $16\varepsilon \equiv 65$, donne $4609 \equiv 0$. Or $4609 = 11.419$: donc 419, qui est *premier* et égal à $2.11.19 + 1$, est le seul facteur θ qui échappe à la démonstration.

Ainsi, en supposant n plus grand que 3, on voit que le cinquième principe est le seul qui donne lieu à de nouvelles exceptions; et les facteurs θ à ajouter au tableau du second livre sont $\theta = 761$ pour $n = 5$, $k = 4$; $\theta = 647$ pour $n = 17$, $k = 1$; $\theta = 419$ pour $n = 11$, $k = 1$, tous trois relatifs à ce dernier cas de $\varphi = 19$.

RÉSUMÉ DE LA PREMIÈRE PARTIE.

Les principes du premier livre ont rendu praticable l'examen des relations $\varepsilon^x + \varepsilon^y + \varepsilon^z \equiv 0$, $\varepsilon^x + \varepsilon^y \equiv \varepsilon^z$, en faisant dépendre la vérification de tous les cas qu'elles comprennent, de celle d'un petit nombre d'entre eux auxquels se ramènent tous les autres. Tels qu'ils sont, et sans qu'il soit nécessaire d'attendre qu'on découvre des formules qui circonscrivent encore davantage le champ de la question, ils rendent le problème abordable, même pour les valeurs de φ au delà de 19. Il n'y a rien du reste à ajouter à leur généralité qui en fait, par cela même, notre meilleure œuvre.

Les principes du second livre démontrent, pour certaines valeurs de z, l'impossibilité des relations $1 + \varepsilon + \varepsilon^z \equiv 0$, $1 + \varepsilon \equiv \varepsilon^z$ auxquelles peuvent toujours se ramener les formules générales $\varepsilon^x + \varepsilon^y + \varepsilon^z \equiv 0$. $\varepsilon^x + \varepsilon^y \equiv \varepsilon^z$. Le premier la démontre pour $z = 1$ et $z = \varphi$; le second pour $z = 2$, $z = \frac{\varphi + 1}{2}$, $z = \varphi - 1$; enfin les deux derniers pour les valeurs

$$z = 3,\quad z = \varphi - 2,\quad z = \frac{m\varphi + 1}{3},\quad z = \frac{m\varphi + 2}{3},\quad z = \frac{\varphi - 1}{2},\quad z = \frac{\varphi + 3}{2}.$$

Là se sont arrêtés nos travaux dans cette voie, mais la route est ouverte, et ce serait un précieux labeur que celui qui étendrait la démons-

tration à quelques-uns des systèmes suivants, quand ce ne serait qu'au premier de ceux-ci, savoir :

$$z=4,\quad z=\varphi-3,\quad z=\frac{m\varphi+1}{4},\quad z=\frac{m\varphi+3}{4},\quad z=\frac{m\varphi-1}{3},\quad z=\frac{m\varphi+4}{3}.$$

Enfin, en appliquant, dans ce troisième livre, les principes des deux premiers, nous avons établi que les relations $1+\varepsilon+\varepsilon^z\equiv 0$, $1+\varepsilon\equiv\varepsilon^z$ sont impossibles, relativement aux nombres *premiers* θ de la forme $2k\varphi n+1$, quel que soit k, pour les valeurs

$$\varphi=5,\quad \varphi=7,\quad \varphi=11,\quad \varphi=13,\quad \varphi=17,\quad \text{et}\quad \varphi=19,$$

n étant un nombre *premier* quelconque plus grand que 2.

Si on prend n plus grand que 3, le nombre déjà fort restreint des facteurs θ qui échappent à notre analyse, se réduit au tableau que nous avons donné dans le second livre, pourvu qu'on y adjoigne les trois exceptions que nous avons données pour le cas de $\varphi=19$.

Avec les mêmes moyens et des artifices semblables, il suffirait sans doute de quelques efforts de plus pour pousser, au delà de $\varphi=19$, les principes de ce dernier livre; et ce serait peut-être ce qu'il y aurait de mieux à faire pour préparer la découverte de la solution générale.

Notre seconde partie, qui comprendra quelques autres principes, établira les progrès que nous avons fait faire à la question depuis l'état où Legendre l'avait laissée en 1825.

NOTES DU SIXIÈME MÉMOIRE.

PREMIÈRE NOTE (*). L'impossibilité de la relation $1+\varepsilon+\varepsilon^z \equiv 0$, dans le cas de $\varphi = 11$, lorsque z a l'une des valeurs 3, 4, 5, 7, 8, et 9, peut se démontrer par un procédé particulier qui n'exige pas la connaissance des principes généraux que nous avons donnés. Exposons le pour $z = 3$.

Si on multiplie $1+\varepsilon+\varepsilon^3 \equiv 0$ par $1+\varepsilon^4+\varepsilon^8+\varepsilon^{10}$, et qu'on ajoute de part et d'autre ε^6, on obtient, après réduction, $2\varepsilon^{11} \equiv \varepsilon^6$ d'où $2^{11} \equiv 1$ résultat dont l'impossibilité s'établirait comme à la page 4 du second livre (**).

Quant à l'absurdité de la relation $1+\varepsilon \equiv \varepsilon^z$ pour les mêmes valeurs de z, nous la démontrerons seulement pour $z = 3$, $z = 4$, $z = 5$, les mêmes procédés réussissant pour les autres valeurs de z, et, d'ailleurs, le second principe du premier livre, facile à établir, nous dispensant de nous livrer à ce travail.

(*) Cette note a été annoncée, à la page 4.

(**) Pour appliquer le même procédé aux autres valeurs de z, il faudra multiplier

$1+\varepsilon+\varepsilon^4 \equiv 0$ par $1+\varepsilon^2+\varepsilon^5+\varepsilon^6$; $1+\varepsilon+\varepsilon^5 \equiv 0$ par $1+\varepsilon^2+\varepsilon^3+\varepsilon^9$;
$1+\varepsilon+\varepsilon^7 \equiv 0$ par $1+\varepsilon^2+\varepsilon^4+\varepsilon^{10}$; $1+\varepsilon+\varepsilon^8 \equiv 0$ par $1+\varepsilon^2+\varepsilon^7+\varepsilon^8$;
$1+\varepsilon+\varepsilon^9 \equiv 0$ par $1+\varepsilon^4+\varepsilon^5+\varepsilon^7$;

et réduire après avoir complété la série, ce qui conduira à $2^{11} \equiv 1$.

Pour les trois autres valeurs de z, savoir 2, 6 et 10, on trouvera $2 \equiv 0$, si on multiplie $1+\varepsilon+\varepsilon^6 \equiv 0$ par $1+\varepsilon^2+\varepsilon^4$; $1+\varepsilon+\varepsilon^2 \equiv 0$ par $1+\varepsilon^3+\varepsilon^6$; $1+\varepsilon+\varepsilon^{10} \equiv 0$ par $\varepsilon+\varepsilon^4+\varepsilon^7$.

Première hypothèse $z = 3$. Si on forme la quatrième puissance de $1 + \varepsilon \equiv \varepsilon^3$, et qu'on réduise, on trouve $\varepsilon^{10} + \varepsilon^7 + \varepsilon^4 + \varepsilon^{11} \equiv 0$, résultat qui, à cause de $\varepsilon^{10} + \varepsilon^{11} \equiv \varepsilon^2$, devient $\varepsilon^2 + \varepsilon^4 + \varepsilon^7 \equiv 0$.

Deuxième hypothèse $z = 4$. Le cube de $1 + \varepsilon \equiv \varepsilon^4$, donne, après réduction, $\varepsilon^9 + \varepsilon^5 + 1 \equiv 0$.

Troisième hypothèse $z = 5$. En formant la huitième puissance de $1 + \varepsilon \equiv \varepsilon^5$, on trouve $\varepsilon^8 + \varepsilon^{11} + \varepsilon^4 + \varepsilon^8 + \varepsilon + \varepsilon^5 + \varepsilon^9 + \varepsilon^2 \equiv 0$. Ce résultat se réduit d'abord à $\varepsilon^2 + \varepsilon^5 + \varepsilon^9 + \varepsilon^8 + \varepsilon^2 \equiv 0$, à cause des diverses relations $\varepsilon^8 + \varepsilon^9 \equiv \varepsilon^2$, $\varepsilon^{11} + \varepsilon \equiv \varepsilon^5$, $\varepsilon^4 + \varepsilon^5 \equiv \varepsilon^9$; il devient définitivement $3\varepsilon^2 + \varepsilon^5 \equiv 0$.

Les résultats, qui se rapportent aux deux premières hypothèses, rentrent dans la forme générale $\varepsilon^x + \varepsilon^y + \varepsilon^z \equiv 0$ dont l'impossibilité est acquise; pour le troisième $3\varepsilon^2 + \varepsilon^5 \equiv 0$, il conduit à $3^{11} \equiv -1$ ou $177148 \equiv 0$. Or 177148, qui est égal à $2.2.67.661$, ne saurait être un multiple de $2k\varphi n + 1$, pour $\varphi = 11$, qu'en supposant $n = 1$, $n = 2$, $n = 3$ ou $n = 5$. Pour le premier et le troisième cas, il y aurait deux facteurs $\theta = 67$, $\theta = 661$ qui resteraient exceptés; quant au second et au quatrième, l'absurdité ne serait contestable que pour un seul facteur $\theta = 661$. On a, en effet, $67 = 2.3.11 + 1$, et $661 = 2.2.3.5.11 + 1$.

Mais on peut faire disparaître cette dernière exception. Dans ce but, mettons $3\varepsilon^2 + \varepsilon^5 \equiv 0$ sous la forme $\varepsilon^3 \equiv -3$, et formons les puissances de cette expression, afin de trouver les éléments pour éliminer avec $1 + \varepsilon \equiv \varepsilon^5$. Ces puissances sont $\varepsilon^6 \equiv 9$ ou $9\varepsilon^5 \equiv 1$; $\varepsilon^9 \equiv -27$; $\varepsilon \equiv 81 \ldots$; et les valeurs numériques de $9\varepsilon^5$ et de ε conduisent facilement à $737 \equiv 0$. Or $737 = 11.67$: il n'y a donc pas d'exception pour n plus grand que 3.

Nous mentionnerons, en terminant cette note, deux formules qui donnent tout réduit le résultat auquel conduit $(1 + \varepsilon)^m \equiv \varepsilon^{mz}$, toutes les fois que m satisfait à l'une des deux conditions $mz = \varphi l + 1$, $mz = \varphi l + m - 1$. Cette réduction offre cela de remarquable que les divers coefficients du résultat sont tous égaux à l'unité.

Ces formules, qui sont

$$\varepsilon^{(m-1)z+1} + \varepsilon^{(m-2)z+1} + \varepsilon^{(m-3)z+1} + \ldots\ldots + \varepsilon^{2z+1} + \varepsilon^{z+1} + 1 \equiv 0,$$
$$\varepsilon^{m} \qquad + \varepsilon^{z+m-2} + \varepsilon^{2z+m-3} + \ldots + \varepsilon^{(m-2)z+1} + \varepsilon^{(m-1)z} \equiv 0,$$

donnent immédiatement, pour $\varphi = 11$, les développements précédents $(1+\varepsilon)^4 \equiv \varepsilon^{3.4}$, $(1+\varepsilon)^3 \equiv \varepsilon^{4.3}$, $(1+\varepsilon)^8 \equiv \varepsilon^{5.8}$, la condition $mz = \varphi l + 1$ étant satisfaite par les deux premières relations, et la troisième satisfaisant à la condition $mz = \varphi l + m - 1$.

Ces expressions peuvent se vérifier à posteriori, soit généralement, soit en attribuant à m et à z des valeurs particulières. Mais on peut les déduire directement de $1 + \varepsilon \equiv \varepsilon^z$, sans recourir au binôme de Newton.

En effet, pour le premier cas $mz \equiv 1$, mettons $1 + \varepsilon \equiv \varepsilon^z$ ou $1 + \varepsilon^{mz} \equiv \varepsilon^z$ sous la forme $1 + \varepsilon^z(\varepsilon^{(m-1)z} - 1) \equiv 0$, et divisons le facteur binôme par $\varepsilon^z - 1$, avec le soin de multiplier son coefficient ε^z par ε, puisque $\varepsilon^z - 1 \equiv \varepsilon$: nous trouvons

$$1 + \varepsilon^{z+1}(\varepsilon^{(m-2)z} + \varepsilon^{(m-3)z} + \ldots + \varepsilon^z + 1) \equiv 0,$$

ou

$$\varepsilon^{(m-1)z+1} + \varepsilon^{(m-2)z+1} \qquad + \ldots + \varepsilon^{2z+1} + \varepsilon^{z+1} + 1 \equiv 0.$$

Pour le deuxième cas $mz \equiv m - 1$, on peut mettre $1 + \varepsilon \equiv \varepsilon^z$ sous la forme $\varepsilon^{m-1} + \varepsilon^m \equiv \varepsilon^{z+m-1}$ ou $\varepsilon^m + \varepsilon^{mz} \equiv \varepsilon^{z+m-1}$, et $\varepsilon^m + \varepsilon^{z+m-1}(\varepsilon^{(m-1)(z-1)} - 1) \equiv 0$. Si alors on divise le facteur binôme par $\varepsilon^{z-1} - 1$, et qu'on multiplie son coefficient par ε^{-1}, à cause de $\varepsilon^{z-1} - 1 \equiv \varepsilon^{-1}$, on trouvera

$$\varepsilon^m + \varepsilon^{z+m-2}(\varepsilon^{(m-2)(z-1)} + \varepsilon^{(m-3)(z-1)} + \ldots + \varepsilon^{2(z-1)} + \varepsilon^{z-1} + 1) \equiv 0,$$

ou, en renversant l'ordre des termes dans le produit effectué,

$$\varepsilon^m + \varepsilon^{z+m-2} + \varepsilon^{2z+m-3} + \ldots + \varepsilon^{(m-2)z+1} + \varepsilon^{(m-1)z} \equiv 0.$$

Deuxième note (1). Les artifices particuliers peuvent dispenser des principes 3 et 4 du second livre.

Ainsi l'impossibilité de $1 + \varepsilon + \varepsilon^z \equiv 0$, pour l'une des valeurs 3, 5, 6,

(*) Cette note a été annoncée, à la page 5.

8, 9, et 11, dans le cas de $\varphi = 13$, dépendant de celle de $1 + \varepsilon + \varepsilon^3 \equiv 0$, peut se démontrer comme il suit :

En cubant $1 + \varepsilon^3 \equiv -\varepsilon$, on obtient $\varepsilon^9 - 3\varepsilon^4 \equiv -(\varepsilon^3 + 1)$ ou $\varepsilon^9 - 3\varepsilon^4 \equiv \varepsilon$. Si on cube de nouveau, on arrive à $\varepsilon - 27\varepsilon^{12} \equiv \varepsilon^3 + 9\varepsilon$ d'où $7\varepsilon + 27\varepsilon^{12} \equiv 1$, c'est-à-dire $7\varepsilon^2 + 27 \equiv \varepsilon$. Éliminant alors ε^2 avec $\varepsilon^2 + 1 \equiv -\varepsilon^{12}$, on trouve $20 \equiv \varepsilon + 7\varepsilon^{12}$ ou $20\varepsilon \equiv \varepsilon^2 + 7$. Éliminant de nouveau ε^2, on obtient $20\varepsilon \equiv 6 - \varepsilon^{12}$ résultat qu'il faut combiner avec $20 \equiv 7\varepsilon^{12} + \varepsilon$, pour faire disparaître successivement ε^{12} et ε. Multipliant alors entre elles les deux relations $139\varepsilon \equiv 22$, $139\varepsilon^{12} \equiv 394$ auxquelles on est conduit, on a $10653 \equiv 0$. Or 10653, qui est égal à $3.53.67$, ne saurait être un multiple de $2k\varphi\pi + 1$ pour $\varphi = 13$, qu'en posant $n = 1$ ou $n = 2$ et $\theta = 53$. Nous sommes arrivé à ce même facteur 53, par une voie bien différente, à la page 12 du second livre.

Quant à l'absurdité de $1 + \varepsilon \equiv \varepsilon^z$ pour les mêmes valeurs de z, il suffit de la démontrer pour $z = 3$, $z = 5$, et $z = 6$.

Première hypothèse $z = 3$. Nous avons deux moyens.

Premier moyen. Formez la puissance cinquième de $1 + \varepsilon \equiv \varepsilon^3$, et réduisez : vous trouverez $\varepsilon^3 + \varepsilon^8 + \varepsilon^{10} \equiv 0$ ou $1 + \varepsilon^5 + \varepsilon^7 \equiv 0$ (*). Ce dernier résultat devient $1 + \varepsilon' + \varepsilon'^4 \equiv 0$, si on pose $\varepsilon^5 \equiv \varepsilon'$ d'où $\varepsilon \equiv \varepsilon'^8$. Si on posait $\varepsilon^7 \equiv \varepsilon'$ d'où $\varepsilon \equiv \varepsilon'^2$, on obtiendrait $1 + \varepsilon' + \varepsilon'^{10} \equiv 0$. Or on démontrerait l'impossibilité de ces relations, comme à la page 5.

Le même procédé réussit pour $1 + \varepsilon \equiv \varepsilon^{11}$, parce que $\varepsilon^{11.5} \equiv \varepsilon^3$.

Deuxième moyen. En partant de $1 + \varepsilon \equiv \varepsilon^3$, on pose $\varepsilon \equiv \varepsilon'^7$ d'où $\varepsilon^3 \equiv \varepsilon'^8$, ce qui donne $1 + \varepsilon^7 \equiv \varepsilon^8$, si on supprime l'accent, ou $1 \equiv \varepsilon^5 + \varepsilon^{12}$. Si alors on ajoute la série dans le premier membre, et qu'on réduise, on trouve

---

(*) Voici le développement :

$$\varepsilon^5 + 5\varepsilon^4 + 10\varepsilon^3 + 9\varepsilon^2 + 5\varepsilon + 1 \equiv 0, \quad \varepsilon^7 + 4\varepsilon^6 + 6\varepsilon^5 + 3\varepsilon^4 + \varepsilon^3 + \varepsilon \equiv 0,$$
$$\varepsilon^9 + 3\varepsilon^8 + 3\varepsilon^7 + \varepsilon^3 + \varepsilon \equiv 0, \quad \varepsilon^{11} + 2\varepsilon^{16} + \varepsilon^7 + \varepsilon^3 + \varepsilon \equiv 0,$$
$$1 + \varepsilon^{10} + \varepsilon^7 + \varepsilon^3 + \varepsilon \equiv 0, \quad 1 + \varepsilon + \varepsilon^3 + \varepsilon^4 + \varepsilon^5 + \varepsilon^{10} \equiv 0,$$
$$1 + \varepsilon + \varepsilon^5 + \varepsilon^6 + \varepsilon^{10} \equiv 0, \quad \varepsilon^3 + \varepsilon^8 + \varepsilon^{10} \equiv 0.$$

$$1 + 1 + \varepsilon + \varepsilon^2 + \varepsilon^3 + \varepsilon^4 + \varepsilon^6 + \varepsilon^7 + \varepsilon^8 + \varepsilon^9 + \varepsilon^{10} + \varepsilon^{11} \equiv 0,$$

ou

$$(1 + \varepsilon + \varepsilon^4)(1 + \varepsilon^2 + \varepsilon^7 + \varepsilon^9) \equiv 0,$$

résultat qui ne peut avoir lieu que si l'on a $1 + \varepsilon^2 + \varepsilon^7 + \varepsilon^9 \equiv 0$, puisque $1 + \varepsilon + \varepsilon^4 \equiv 0$ est démontré absurde. Or $1 + \varepsilon^2 + \varepsilon^7 + \varepsilon^9 \equiv 0$ revient à $(1 + \varepsilon^2)(1 + \varepsilon^7) \equiv 0$, et est par conséquent impossible.

Si on partait de $1 + \varepsilon \equiv \varepsilon^{11}$, il faudrait poser $\varepsilon \equiv \varepsilon'^6$, et on arriverait au même résultat.

Pour avoir la clef de ce calcul, il faut multiplier $1 + \varepsilon + \varepsilon^4 \equiv 0$ par $1 + \varepsilon^2 + \varepsilon^7 + \varepsilon^9$, ce qui donne, après réduction, $1 \equiv \varepsilon^5 + \varepsilon^{12}$ relation qui peut être mise sous la forme $\varepsilon^8 \equiv 1 + \varepsilon^7$ ou $\varepsilon \equiv \varepsilon^6 + 1$. Or le premier résultat devient $1 + \varepsilon' \equiv \varepsilon'^3$, si on pose $\varepsilon^7 \equiv \varepsilon'$; et le second devient $1 + \varepsilon' \equiv \varepsilon'^{11}$, si on fait $\varepsilon^6 \equiv \varepsilon'$.

Deuxième hypothèse $z = 5$. Si on cube $1 + \varepsilon \equiv \varepsilon^5$, on trouve $\varepsilon^3 + 2\varepsilon^2 + 3\varepsilon + 1 \equiv 0$, $\varepsilon^3 + 2\varepsilon^6 + \varepsilon^5 \equiv 0$, $\varepsilon^3 + \varepsilon^6 + \varepsilon^{10} \equiv 0$, $1 + \varepsilon^3 + \varepsilon^7 \equiv 0$ qui devient $1 + \varepsilon' + \varepsilon'^{11} \equiv 0$, si on pose $\varepsilon^3 \equiv \varepsilon'$, et $1 + \varepsilon' + \varepsilon'^6 \equiv 0$ si on fait $\varepsilon^7 \equiv \varepsilon'$, formes dont l'absurdité est acquise.

Troisième hypothèse $z = 6$. Le cube de $1 + \varepsilon \equiv \varepsilon^6$ donne $1 + \varepsilon^3 \equiv \varepsilon^5 - 3\varepsilon^7$; mais $3\varepsilon^7 + 3\varepsilon^8 \equiv 3$: donc $4 + \varepsilon^3 \equiv \varepsilon^5 + 3\varepsilon^8$ ou $4\varepsilon^5 + \varepsilon^8 \equiv \varepsilon^{10} + 3$. Ainsi, en carrant, on aura successivement $10\varepsilon^{10} + \varepsilon^3 \equiv \varepsilon^7 + 1$, $98\varepsilon^7 + \varepsilon^6 \equiv \varepsilon + 1 - 20$ ou $49\varepsilon^7 \equiv -10$, puis $49\varepsilon^6 \equiv -10\varepsilon^{12}$.

Éliminant ε^{12} avec $\varepsilon^6 + \varepsilon^7 \equiv \varepsilon^{12}$, on trouve $59\varepsilon^6 + 10\varepsilon^7 \equiv 0$.

Éliminant ε^7, on a $49.59\varepsilon^6 \equiv 100$, et, par suite, $49.49.59 \equiv -1000$ ou $142659 \equiv 0$. Or ce nombre est égal à $3.3.11.11.131$, et ne saurait être un multiple de $2k\varphi n + 1$, pour $\varphi = 13$ (n ne pouvant être égal à 1), que si on suppose $n = 5$; encore pour cette valeur de n, un seul facteur serait excepté, savoir $\theta = 131$.

Par ces moyens et d'autres semblables, nous étions parvenu à démontrer l'impossibilité des relations $1 + \varepsilon + \varepsilon^z \equiv 0$, $1 + \varepsilon \equiv \varepsilon^z$ pour $\varphi = 11$ et pour $\varphi = 13$, avant d'avoir découvert les principes généraux exposés dans cet ouvrage. Nous avons tenu à conserver ces démonstrations, par le souvenir des efforts qu'ils nous ont coûtés, et pour ne rien perdre des procédés tant que le problème n'est pas résolu.

Troisième note (*). Voici le développement de la septième puissance de $1+\varepsilon\equiv\varepsilon^4$, dans l'hypothèse de $\varphi=13$. Les réductions s'opèrent d'une relation à l'autre, et s'appuient sur les diverses formes de $1+\varepsilon\equiv\varepsilon^4$.

$$\begin{array}{l}
\varepsilon^7+7\varepsilon^6+21\varepsilon^5+35\varepsilon^4+35\varepsilon^3+21\varepsilon^2+7\varepsilon+1\equiv\varepsilon^2;\\
\varepsilon^{10}+6\varepsilon^9+15\varepsilon^8+20\varepsilon^7+15\varepsilon^6+5\varepsilon^5+\varepsilon^4+\varepsilon\equiv 0;\\
1+5\varepsilon^{12}+10\varepsilon^{11}+10\varepsilon^{10}+5\varepsilon^9+\varepsilon^4+\varepsilon\equiv 0;\\
\varepsilon^3+4\varepsilon^2+6\varepsilon+4+\varepsilon^9+\varepsilon^4+\varepsilon\equiv 0;\\
\varepsilon^6+3\varepsilon^5+3\varepsilon^4+1+\varepsilon^9+\varepsilon^4+\varepsilon\equiv 0;\\
\varepsilon^9+2\varepsilon^8+\varepsilon^4+1+\varepsilon^9+\varepsilon^4+\varepsilon\equiv 0;\\
\varepsilon^{12}+\varepsilon^8+\varepsilon^4+1+\varepsilon^9+\varepsilon^4+\varepsilon\equiv 0.
\end{array}$$

Quatrième note (**). Le second mode d'examen conduit également au but, et donne lieu à des calculs assez heureux. Nous allons donner ces calculs.

Il s'agit d'examiner, dans l'hypothèse de $\varphi=17$, la possibilité des relations

$$1+\varepsilon\equiv\varepsilon^4,\qquad \varepsilon-1\equiv\varepsilon^4,\qquad \varepsilon-1\equiv-\varepsilon^4.$$

La première de ces relations n'est autre que celle dont nous nous sommes occupé, à la page 7. Restent donc seulement les deux autres relations qui correspondent, la première, aux deux formes $1+\varepsilon\equiv\varepsilon^5$, $1+\varepsilon\equiv\varepsilon^{13}$, la seconde, aux deux formes $1+\varepsilon\equiv\varepsilon^7$, $1+\varepsilon\equiv\varepsilon^{11}$, déjà examinées les unes et les autres, aux pages 8 et 9 (***).

1° Si on développe la cinquième puissance de $\varepsilon-1\equiv\varepsilon^4$, on trouve

$$\begin{array}{l}
\varepsilon^5-5\varepsilon^4+9\varepsilon^3-10\varepsilon^2+5\varepsilon-1\equiv 0;\\
\varepsilon^8-\varepsilon^4-3\varepsilon^7+6\varepsilon^6-4\varepsilon^5+\varepsilon^4\equiv 0;\\
\varepsilon^8-\varepsilon^4-3\varepsilon^{10}+3\varepsilon^9-\varepsilon^8\equiv 0;\\
-\varepsilon^4-3\varepsilon^{13}\equiv 0;
\end{array}$$

ce qui donne, comme à la page 8, $3^{17}\equiv-1$. Mais on évite facilement la considération de cette puissance. On a, en effet, successivement

(*) Cette note a été annoncée, à la page 5.

(**) Cette note a été annoncée, à la page 7.

(***) On passe, en effet, de $\varepsilon-1\equiv\varepsilon^4$ à $1+\varepsilon'\equiv\varepsilon'^{13}$ en posant $\varepsilon^4\equiv\varepsilon'$, et de $\varepsilon-1\equiv-\varepsilon^4$ mis sous la forme $1+\varepsilon^3\equiv\varepsilon^{16}$, à $1+\varepsilon'\equiv\varepsilon'^{11}$, en posant $\varepsilon^3\equiv\varepsilon'$. On déduirait aussi facilement des proposées, les formes $1+\varepsilon\equiv\varepsilon^5$, $1+\varepsilon\equiv\varepsilon^7$.

$3\varepsilon^9 \equiv -1$ ou $\varepsilon^8 \equiv -3$; et $9\varepsilon \equiv 1$. Ainsi $9\varepsilon - 9 \equiv 9\varepsilon^4$ deviendra $9\varepsilon^4 \equiv -8$, et par conséquent $81\varepsilon^8 \equiv 64$ qui, comparé à $81\varepsilon^8 \equiv -243$, conduira à $307 \equiv 0$.

2° Si on forme la sixième puissance de $\varepsilon - 1 \equiv -\varepsilon^4$, on peut réduire de manière à obtenir $3\varepsilon^8 + \varepsilon^9 \equiv 2$ (*). On en tire, en carrant, $9\varepsilon^{16} + \varepsilon \equiv -2$ qui peut prendre les deux autres formes $9 + \varepsilon^2 \equiv -2\varepsilon$, $9\varepsilon + \varepsilon^3 \equiv -2\varepsilon^2$, et qui, combiné avec $\varepsilon^{16} - 1 \equiv \varepsilon^3$, donne $11 + \varepsilon \equiv -9\varepsilon^3$. Cette dernière expression sert à éliminer ε^3 avec $9\varepsilon + \varepsilon^3 \equiv -2\varepsilon^2$, et le résultat $80\varepsilon - 11 \equiv -18\varepsilon^2$ sert, à son tour, à éliminer ε^2 avec $9 + \varepsilon^2 \equiv -2\varepsilon$, ce qui donne $173 \equiv 44\varepsilon$. On trouve alors facilement $261 \equiv -396\varepsilon^{16}$ et $62577 \equiv 0$. Or $62577 \equiv 3.3.17.409$.

Cinquième note (**). Le développement de la puissance cinquième de $1 + \varepsilon \equiv \varepsilon^4$, dans l'hypothèse de $\varphi = 17$, donne lieu au calcul suivant :

$$\begin{aligned}
&\varepsilon^5 + 5\varepsilon^4 + 10\varepsilon^3 + 10\varepsilon^2 + 5\varepsilon + 1 \equiv \varepsilon^3;\\
&\varepsilon^5 + 5\varepsilon^4 + 9\varepsilon^3 + 10\varepsilon^2 + 5\varepsilon + 1 \equiv 0;\\
&\varepsilon^4 + \varepsilon^8 + 3\varepsilon^7 + 6\varepsilon^6 + 4\varepsilon^5 + \varepsilon^4 \equiv 0;\\
&\varepsilon^4 + \varepsilon^8 + 3\varepsilon^{10} + 3\varepsilon^9 + \varepsilon^8 \equiv 0;\\
&\varepsilon^4 + \varepsilon^8 + 3\varepsilon^{13} + \varepsilon^8 \equiv 0;\\
&\varepsilon^4 + 2\varepsilon^8 + 3\varepsilon^{13} \equiv 0.
\end{aligned}$$

Le développement pourrait conduire à un autre résultat qui, réuni au précédent, résoudrait fort simplement la difficulté. On développerait alors

---

(*) Le développement est d'abord

$$\varepsilon^6 - 6\varepsilon^5 + 15\varepsilon^4 - 20\varepsilon^3 + 15\varepsilon^2 - 6\varepsilon + 1 \equiv \varepsilon^7.$$

Si on opère alors les réductions, on trouve successivement pour les premiers membres des relations :

$$\begin{aligned}
&-\varepsilon^9 + 5\varepsilon^8 - 11\varepsilon^7 + 10\varepsilon^6 - 5\varepsilon^5 + \varepsilon^4; \quad -\varepsilon^9 - 5\varepsilon^{11} + 6\varepsilon^{10} - 4\varepsilon^9 + \varepsilon^8;\\
&-\varepsilon^9 - 2\varepsilon^{10} + 3\varepsilon^{14} - 3\varepsilon^{13} + \varepsilon^{12}; \quad -\varepsilon^9 - 2\varepsilon^{10} + \varepsilon^{14} - 2 + \varepsilon^{16};\\
&-\varepsilon^9 - 2\varepsilon^{11} + \varepsilon^{14} - 1 + \varepsilon^3; \quad -\varepsilon^9 - 3\varepsilon^{11} + \varepsilon^{10} - 1 + \varepsilon^3;\\
&-3\varepsilon^{11} - \varepsilon^{13} - 1 + \varepsilon^3; \quad -3\varepsilon^{11} - \varepsilon^{12} + \varepsilon^{16} - 1 + \varepsilon^3;\\
&-3\varepsilon^{11} - \varepsilon^{12} + 2\varepsilon^3; \quad \text{et } -3\varepsilon^8 - \varepsilon^9 + 2.
\end{aligned}$$

Pour abréger, nous avons supprimé le signe $\equiv$ et le second membre qui est zéro dans toutes ces relations.

(**) Cette note a été annoncée, à la page 7.

de la manière suivante :

$$\begin{aligned}
&\varepsilon^5 + 5\varepsilon^4 + 9\varepsilon^3 + 10\varepsilon^2 + 5\varepsilon + 1 \equiv 0;\\
&\varepsilon^8 + 4\varepsilon^7 + 5\varepsilon^6 + 5\varepsilon^5 + 1 \equiv 0;\\
&\varepsilon^{11} + 3\varepsilon^{10} + 2\varepsilon^9 + 3\varepsilon^5 + 1 \equiv 0;\\
&\varepsilon^{14} + 2\varepsilon^{13} + 3\varepsilon^5 + 1 \equiv 0;\\
&1 + \varepsilon^{13} + 3\varepsilon^5 + 1 \equiv 0;\\
&\varepsilon^{13} + 3\varepsilon^5 + 2 \equiv 0.
\end{aligned}$$

Pour éliminer ε^5 de ce dernier résultat, on déduit successivement de $\varepsilon^4 + 2\varepsilon^8 + 3\varepsilon^{13} \equiv 0$, en ayant égard à $\varepsilon^8 \equiv \varepsilon^4 + \varepsilon^5$, les relations $3\varepsilon^4 + 2\varepsilon^5 + 3\varepsilon^{13} \equiv 0$, ou $9\varepsilon^4 + 6\varepsilon^5 + 9\varepsilon^{13} \equiv 0$; $9\varepsilon^4 + 9\varepsilon^{13} \equiv 2\varepsilon^{13} + 4$; $9\varepsilon^4 + 7\varepsilon^{13} \equiv 4$. Et, pour éliminer ε^8, on obtient $9\varepsilon^8 + 7 \equiv 4\varepsilon^4$, $18\varepsilon^8 + 14 \equiv 8\varepsilon^4$, $14 \equiv 8\varepsilon^4 + 9\varepsilon^4 + 27\varepsilon^{13}$, $17\varepsilon^4 + 27\varepsilon^{13} \equiv 14$. Il ne reste plus qu'à éliminer entre celle-ci et $9\varepsilon^4 + 7\varepsilon^{13} \equiv 4$. On trouve $62\varepsilon^{13} \equiv 29$, $62\varepsilon^4 \equiv 5$, et par conséquent $3699 \equiv 0$. Or $3699 \equiv 3.3.3.137$ ce qui conduit à la même condition numérique $137 \equiv 0$.

Sixième note (*). Voici comment on peut faire le développement de la puissance cinquième de $1 + \varepsilon \equiv \varepsilon^7$, dans l'hypothèse de $\varphi = 17$:

$$\begin{aligned}
&\varepsilon^5 + 5\varepsilon^4 + 10\varepsilon^3 + 10\varepsilon^2 + 5\varepsilon + 1 \equiv \varepsilon;\\
&\varepsilon^{11} + 4\varepsilon^{10} + 6\varepsilon^9 + 4\varepsilon^8 + \varepsilon + 1 \equiv \varepsilon;\\
&1 + 3\varepsilon^{16} + 3\varepsilon^{15} + \varepsilon^8 + 1 \equiv 0;\\
&3\varepsilon^5 + \varepsilon^8 + 2 \equiv 0.
\end{aligned}$$

Septième note (**). Le développement de la puissance sixième de $1 + \varepsilon \equiv \varepsilon^4$, dans l'hypothèse de $\varphi = 19$, peut s'opérer ainsi :

$$\begin{aligned}
&\varepsilon^6 + 6\varepsilon^5 + 15\varepsilon^4 + 20\varepsilon^3 + 15\varepsilon^2 + 6\varepsilon + 1 \equiv \varepsilon^5;\\
&\varepsilon^9 + 4\varepsilon^8 + 11\varepsilon^7 + 9\varepsilon^6 + 6\varepsilon^5 + 1 \equiv 0;\\
&\varepsilon^{12} + 3\varepsilon^{11} + 8\varepsilon^{10} + \varepsilon^9 + 5\varepsilon^5 + 1 \equiv 0;\\
&\varepsilon^{15} + 2\varepsilon^{14} + \varepsilon^{13} + 5\varepsilon^{10} + 5\varepsilon^5 + 1 \equiv 0;\\
&\varepsilon^{18} + \varepsilon^{17} + 5\varepsilon^{10} + 5\varepsilon^5 + 1 \equiv 0;\\
&5\varepsilon^{10} + 5\varepsilon^5 + \varepsilon^2 + 1 \equiv 0.
\end{aligned}$$

(*) Cette note a été annoncée, à la page 8.

(**) Cette note a été annoncée, à la page 10.

Huitième note (*). On peut effectuer, comme il suit, dans l'hypothèse de $\varphi = 19$, le développement de la puissance cinquième de $1 + \varepsilon \equiv \varepsilon^8$:

$$\begin{aligned}
&\varepsilon^5 + 5\varepsilon^4 + 10\varepsilon^3 + 10\varepsilon^2 + 5\varepsilon + 1 \equiv \varepsilon^2;\\
&\varepsilon^5 + 5\varepsilon^4 + 10\varepsilon^3 + 9\varepsilon^2 + 5\varepsilon + 1 \equiv 0;\\
&\varepsilon^{12} + 4\varepsilon^{11} + 6\varepsilon^{10} + 3\varepsilon^9 + \varepsilon^8 + \varepsilon \equiv 0;\\
&1 + 3\varepsilon^{18} + 3\varepsilon^{17} + \varepsilon^8 + \varepsilon \equiv 0;\\
&1 + 3\varepsilon^6 + \varepsilon^8 + \varepsilon \equiv 0;\\
&3\varepsilon^6 + 2\varepsilon^8 \equiv 0.
\end{aligned}$$

(*) Cette note a été annoncée, à la page 13.

Paris. — Typographie de Firmin Didot frères, fils et Ce, rue Jacob, 56.

SEPTIÈME MÉMOIRE

SUR

LA THÉORIE DES NOMBRES,

PAR M. F. LANDRY.

Décembre 1859.

BIBLIOTHÈQUE

PROCÉDÉS NOUVEAUX

POUR DÉMONTRER QUE

Le nombre 2 147 483 647 est *premier*.

PARIS,
LIBRAIRIE DE L. HACHETTE ET Cie,
RUE PIERRE-SARRAZIN, N° 14.
1859.

OUVRAGES DÉJA PUBLIÉS.

Premier mémoire, sur un théorème de Legendre. Février 1853.

Second mémoire, Recherches nouvelles sur le théorème de Fermat. Premier livre. Juillet 1853.

Troisième mémoire, Nouvelle méthode pour la détermination des *racines primitives*. Mars 1854.

Table des nombres *premiers*, de 1 à 10000. Février 1855.

Table des nombres entiers non divisibles par 2, 3, 5 et 7, jusqu'à 10201, avec leurs diviseurs simples en regard, et des carrés des 1000 premiers nombres. Février 1855.

Quatrième mémoire, deuxième livre des Recherches nouvelles sur le théorème de Fermat. Février 1855.

Cinquième mémoire, Théorème sur les réduites d'une nouvelle espèce de fractions *continues*. Juillet 1855.

Sixième mémoire, troisième et dernier livre des Recherches nouvelles sur le théorème de Fermat. Novembre 1856.

PROCÉDÉS NOUVEAUX

POUR DÉMONTRER QUE

Le nombre 2 147 483 647 est *premier*.

Nous nous sommes proposé de rechercher, après Euler (car Legendre n'a pas abordé le calcul, et s'est borné à faire connaître les travaux de son illustre devancier), si le nombre $2^{31} - 1$ ou 2147483647 est *premier* (*). Ce n'est pas qu'il nous parût d'un grand intérêt de confirmer un résultat annoncé par une aussi grande autorité, après l'assertion de Fermat; mais ces recherches conduisent quelquefois à des procédés qui peuvent ensuite s'appliquer utilement, surtout à de moindres nombres. La science gagne toujours quelque chose, même au défrichement de ses parties les plus arides. Telle est la pensée qui nous a soutenu dans ce labeur, essayé à plusieurs reprises, sans que les moyens particuliers auxquels nous avons eu recours nous aient encore donné une bien complète satisfaction.

Dans cette recherche, Legendre (*Théorie des Nombres*, page 197, seconde édition) nous conduit, comme résultat des méthodes qu'il expose d'après Euler, et nous laisse à ce point, que, si le nombre $2^{31} - 1$ que nous désignerons par N, n'est pas *premier*, ses facteurs simples ne peu-

(*) Gauss, qui s'est occupé toute sa vie de ces théories délicates, n'a point, à notre connaissance, appliqué ses méthodes à la vérification de ce nombre *premier*.

vent être que de l'une des deux formes $248x+1$, $248x+63$. Cette double forme provient de la forme $62x+1$ propre aux diviseurs des nombres $\frac{a^{31}-1}{a-1}$ et des deux formes $8n+1$, $8n+7$ appartenant aux diviseurs des nombres t^2-2, car $2N$ ou $2^{32}-2$ est de la forme t^2-2.

On pourrait ajouter que N ne peut avoir plus de deux facteurs, et que ces deux facteurs, s'ils existent, sont l'un de la forme $248x+1$, l'autre de la forme $248x+63$. D'abord les formes assignées aux facteurs *premiers* de N dont la racine quatrième est inférieure à 216, s'opposent à ce qu'il en ait quatre, puisque leurs moindres valeurs (63 excepté) sont supérieures à cette racine; et l'on reconnaît bientôt, ensuite, que, pour une raison semblable, il ne saurait en avoir trois, sa racine cubique étant moindre que 1291. Car, si on développe les deux formules $248x+1$, $248x+63$ jusqu'à cette limite, on trouve les nombres 249, 311, 497, 559, 745, 807, 993, 1055, 1241; et l'on voit qu'en rejetant de ces neuf nombres ceux qui sont multiples de 3, de 5 ou de 7, ainsi que 559 qui est un multiple de 13, et 1241 qui est un multiple de 17 (*), il ne reste définitivement que le seul nombre 311 à essayer comme diviseur. Or la division donne 6905092 pour quotient, et 35 pour reste.

Le nombre N a donc, au plus, deux facteurs, puisqu'il n'en a aucun au-dessous de sa racine cubique; et, comme il est égal à $248.8659208+63$, ces deux facteurs, s'ils existent, doivent être l'un de la forme $248x+1$, l'autre de la forme $248x+63$.

Malgré ces observations, la question resterait la même, faute de savoir dans quelle forme devrait se trouver le plus petit des deux facteurs. On pourrait, il est vrai, se livrer d'abord à cette recherche; mais le calcul nous a paru tout aussi long que celui que nous indiquerons pour résoudre la question elle-même. Ainsi il faudrait, en dehors de cette recherche, comme Euler l'a fait, essayer tous les nombre *premiers* compris dans les formules mentionnées, entre 249 et 46341 nombre entier immédiatement supérieur à la racine carrée de N.

Pour prendre une idée de l'importance du calcul, on observera que

---

(*) $559=13.43$; $1241=17.73$.

46340 est égal à 248.186 plus 212, de sorte qu'il y a au-dessous de la racine carrée de N, 186 nombres de la forme $248x + 1$; et qu'il y en a 187 de la seconde forme $248x + 63$, y compris 63. Il y aurait donc 373 diviseurs à essayer, sauf à rejeter, parmi eux, ceux qui ne sont pas *premiers*, ce qui a l'inconvénient d'exiger une table. On pourrait, toutefois, à défaut de table, retirer de la liste de ces diviseurs tous les multiples de 3 ou de 5, ce qui réduirait le nombre des essais à 198 (*). Si, de plus, on supprimait les multiples de 7, et ceux des nombres restants qui ne sont pas *premiers*, au moins jusqu'à la limite de notre petite table (**), on n'aurait plus qu'à refaire, à très-peu près, le calcul d'Euler. Seulement, même pour l'opérateur, le nombre et la longueur des divisions à effectuer, grâce à la grandeur du dividende N, pourraient bien laisser planer quelques nuages sur la certitude du résultat. On jugera si nous avons remédié, en partie du moins, à ces graves inconvénients.

Considérons les formes les plus simples des facteurs *premiers* de $2^{31} - 1$; et posons, s'il est possible,

$$N = (62x + 1)(62x' + 1),$$

nous trouverons, en effectuant la multiplication,

$$N = 3844\,xx' + 62\,(x + x') + 1.$$

D'un autre côté, $N = 3844.558658 + 62.37 + 1$, expression qui revient à

$$N = 3844\,(558658 - h) + 62\,(62h + 37) + 1.$$

En comparant les deux valeurs de N que nous venons d'obtenir, on formera les deux relations

$$(1) \quad xx' = 558658 - h; \qquad (2) \quad x + x' = 62h + 37.$$

Si maintenant on désigne par t l'une quelconque des deux inconnues x, x', on trouvera sans difficulté

$$(3) \quad 2t = 62h + 37 \pm \sqrt{3844\,h^2 + 4592\,h - 2233263}.$$

(*) Voir la note première, page 14.

(**) Notre petite table va jusqu'à 10 000. Nous la proposons, parce que chacun peut en vérifier l'exactitude en quelques heures.

Dans cette dernière expression, le signe *moins* se rapporte à la plus petite des deux racines, et la valeur de cette racine, du moment qu'elle est réelle, diminue à mesure que h augmente, puisque le produit xx' diminue, et que la valeur de l'autre racine ne cesse d'augmenter. Ainsi il y a une valeur minimum de h qui sépare la suite des valeurs décroissantes de la plus petite des indéterminées, et celle des valeurs croissantes de la plus grande. Cette valeur minimum de h est comprise entre 23 et 24.

Les trois relations (1), (2), (3), qui doivent être vérifiées par des nombres entiers, si l'hypothèse est vraie, imposent aux variables x, x', et h, des formes particulières intéressantes à étudier. Nous nous occuperons ici des formes de h.

Les deux premières relations nous montrent d'abord que h est un nombre pair.

Si maintenant, dans l'expression de t, nous considérons, pour le module 9, le résidu $h^2 + 2h - 3$ de la quantité sous le signe, et qu'on observe que, pour être un carré, cette quantité ne peut être un multiple de 3 qu'à la condition d'être un multiple de 9, on en conclura que les seules formes admissibles pour h qui est pair, sont

$$18h' + 2,\ 18h' + 6,\ 18h' + 8,\ 18h' + 10,\ 18h' + 14.$$

Cela posé, considérons, de nouveau, les deux premières relations (1) et (2); et cherchons les formes de h relatives au module 3. Pour ce module les relations donnent

$$xx' \equiv 1 - h,\quad x + x' \equiv 2h + 1,$$

conditions qui deviennent, pour $h = 3h' + 2$,

$$xx' \equiv 2,\quad x + x' \equiv 2$$

et auxquelles on ne peut satisfaire. En effet, les seules hypothèses, qui conviennent à la première, sont

$$x \equiv 1,\quad x' \equiv 2 \text{ ou } x \equiv 2,\quad x' \equiv 1,$$

ce qui donne $x + x' \equiv 0$, de sorte que la seconde condition ne se trouve

point vérifiée. Ainsi h ne saurait avoir la forme $3h' + 2$. Les formes précédemment trouvées se réduisent donc, par cela même, à deux seulement :

$$18h' + 6, \quad 18h' + 10.$$

Il est à remarquer que toutes deux donnent des multiples de 9 pour la quantité sous le signe.

Les deux mêmes relations (1) et (2) font encore voir que la forme de h, relative au module 5, ne peut être aucune des trois

$$5h', \quad 5h' + 1, \quad 5h' + 2.$$

On a en effet, pour ce module,

$$xx' \equiv 3 - h, \quad x + x' \equiv 2h + 2,$$

relations qui deviennent

$$\begin{aligned} &xx' \equiv 3, \quad x + x' \equiv 2, \quad \text{pour } h = 5h'; \\ &xx' \equiv 2, \quad x + x' \equiv 4, \quad \text{pour } h = 5h' + 1; \\ &xx' \equiv 1, \quad x + x' \equiv 1, \quad \text{pour } h = 5h' + 2. \end{aligned}$$

Ces divers résultats sont impossibles à vérifier, quelque valeur que l'on veuille attribuer aux indéterminées x, x'.

Les seules formes admissibles pour h, relativement au même module, sont donc

$$5h' + 3, \quad 5h' + 4,$$

ou, parce que h est pair,

$$10h' + 4, \quad 10h' + 8.$$

En développant les deux espèces de formes imposées à h, pour les deux modules 18 et 10, on prendra les termes communs aux deux développements, et il n'y aura d'hypothèse à faire pour h que celle des valeurs exprimées par ces termes. Elles sont comprises dans les quatre formules

$$90l + 24, \quad 28, \quad 64, \quad 78.$$

Il ne reste qu'à substituer ces valeurs à h, sous le radical, et à chercher, en faisant varier l, s'il se trouve un carré parmi les nombres obtenus. La quantité sous le signe, débarrassée du facteur commun 9, prend, après

la substitution, à cause des quatre formes de h, les quatre formes que voici :

$$3459600\,l^2 + 1891040\,l + 10121;$$
$$3459600\,l^2 + 2198560\,l + 101001;$$
$$3459600\,l^2 + 4966240\,l + 1533961;$$
$$3459600\,l^2 + 6042560\,l + 2390201.$$

Les nombres à obtenir se formeront les uns des autres, à partir de $l = 0$, à l'aide des différences.

La différence première est

$$6919200\,l + 5350640,\ 5658160,\ 8425840,\ 9502160.$$

La différence seconde est 6919200.

Voici le tableau des valeurs que l'on trouve en développant ces formules depuis $l = 0$ jusqu'à $l = 6$, c'est-à-dire depuis $h = 24, 28, 64, 78$, jusqu'à $h = 564, 568, 604, 618$:

$h = 24$	10121,	$h = 28$	101001,	$h = 64$	1533961,	$h = 78$	2390201;
$h = 114$	5360761,	$h = 118$	5759161,	$h = 154$	9959801,	$h = 168$	11892361;
$h = 204$	17630601,	$h = 208$	18336521,	$h = 244$	25304841,	$h = 258$	28313721;
$h = 294$	36819641,	$h = 298$	37833081,	$h = 334$	47569081,	$h = 348$	51654281;
$h = 384$	62927881,	$h = 388$	64248841,	$h = 424$	76752521,	$h = 438$	81914041;
$h = 474$	95955321,	$h = 478$	97583801,	$h = 514$	112855161,	$h = 528$	119093001;
$h = 564$	135901961,	$h = 568$	137837961,	$h = 604$	155877001,	$h = 618$	163191161.

Si l'on s'assure qu'aucun des nombres, compris au tableau précédent (*), n'est un carré (**), on sera certain que, jusqu'à $h = 618$, il n'existe aucune valeur de t propre à donner un diviseur de N.

La valeur de t, qui correspond à $h = 618$, étant moindre que 16, et continuant à diminuer en même temps que h augmente, il en résulte

(*) Ces nombres ont une vérification importante. Comme ils se déduisent les uns des autres, dans chaque colonne, on pourra vérifier leur exactitude en calculant directement le dernier de chacune d'elles, à l'aide de la quantité sous le signe, dans l'expression de t.

(**) Voir la note seconde, page 15.

que, si N n'est pas *premier*, le plus petit de ses diviseurs $62x+1$ est compris de $x=15$ à $x=1$.

Ces nombres, que voici :

63, 125, 187, 249, 311, 373, 435, 497, 559, 621, 683, 745, 807, 869, 931,

ne contiennent que trois facteurs *premiers*, savoir : 311, 373, 683.

On a, en effet, $187=11.17$; $559=13.43$; $869=11.79$; et tous les autres nombres sont des multiples de 3, de 5 ou de 7. Ainsi, on aurait à diviser N par ces trois facteurs (*).

Mais, si on déduit des relations (1) et (2), par l'élimination de l'une des deux indéterminées x, x', la valeur de h, on pourra remplacer les trois divisions à faire, par trois autres moins laborieuses, en posant, dans cette dernière expression

$$h=\frac{558658-t(37-t)}{62t+1},$$

les trois valeurs de t qui correspondent aux facteurs dont il s'agit, savoir : $t=5$, $t=6$, $t=11$.

Ces substitutions donnent pour h les trois valeurs

$$\frac{558498}{311},\qquad \frac{558472}{373},\qquad \frac{558372}{683}$$

dont aucune n'est un nombre entier (**).

On achève ainsi de démontrer que N est *premier*, sans avoir eu besoin de faire aucun division sur ce nombre.

Cette dernière formule $h=\frac{558658-t(37-t)}{62t+1}$ peut dispenser de pousser, aussi loin que nous l'avons fait, le calcul des quantités sous le signe dans la valeur de t. Nous allons exposer le parti que l'on peut en

---

(*) Il est clair qu'il suffirait de diviser N par 311 (division déjà faite, page 4), si on observe que 373 et 683 ne sont ni de la forme $8n+1$, ni de la forme $8n+7$. Mais nous avons voulu procéder sans recourir à ce principe.

(**) On trouve, en effet, $558\,498=311.1795+253$; $558\,472=373.1497+91$; $558\,372=683.817+361$.

tirer, car c'est une seconde méthode qui abrége la première, et suffit même seule pour conduire au but.

On voit que la formule commence par donner de grandes valeurs de h, pour les premières valeurs 1, 2, 3 ... de l'indéterminée t, et que ces valeurs diminuent, en même temps que l'indéterminée t s'accroît. On a remarqué que, dans l'expression irrationnelle de t, la plus petite des deux indéterminées diminue à mesure que h augmente; ici c'est la valeur de h qui diminue par l'effet des premiers accroissements de t. Ces variations sont d'abord très-rapides; mais bientôt h diminue d'une manière moins sensible; et, plus tard, après être demeuré presque stationnaire dans le voisinage de $h=24$, il cesse de diminuer pour croître indéfiniment. Cela tient à ce que le dividende, qui diminuait d'abord, cesse bientôt de décroître pour augmenter, et finit par croître dans un rapport plus grand que le diviseur. Nous retrouvons ici la valeur minimum de h qui sépare les deux suites des diviseurs conjugués de N, celle des diviseurs moindres que $\sqrt{N}$, et celle des diviseurs plus grands que cette racine.

Dans l'application de la formule, on pourrait n'essayer que les valeurs de t qui donnent pour $62t+1$, des nombres *premiers*, et notre petite table ferait connaître ceux-ci jusqu'à $t=164$. Mais, si l'on veut éviter l'usage d'une table, on pourra toujours supprimer les valeurs de t qui produisent des multiples de 3 ou de 5, ce qui revient à ne conserver pour t que les valeurs particulières comprises dans les formes :

$$15t'+0,\ 3,\ 5,\ 6,\ 8,\ 9,\ 11,\ 14\ (*).$$

Maintenant, si on veut profiter de ce que les diviseurs de N doivent être de l'une des formes $8n+1$, $8n+7$, il suffira de rejeter de la suite précédente les valeurs de t qui ne sont d'aucune des deux formes 4θ, $4\theta+1$, ce qui la réduit à

$$60t'+0,\ 5,\ 8,\ 9,\ 20,\ 21,\ 24,\ 29,\ 33,\ 36,\ 41,\ 44,\ 45,\ 48,\ 53,\ 56\ (**).$$

(*) On pourrait encore exclure les formes $7a+1$ qui donnent des multiples de 7, et les formes $11a+3$ qui donnent des multiples de 11. Mais les exclusions nouvelles seraient en petit nombre, et les formules perdraient de leur simplicité.

(**) Jusqu'à $t=60$, dans cette liste, on peut supprimer les termes 8, 29, et 36, qui donneraient pour $62t+1$ des multiples de 7.

On pourra donc reconnaître, par un petit nombre de divisions, que, jusqu'à $t = 60$, il n'existe aucun diviseur de N, de sorte que si on voulait, pour terminer, employer la méthode des carrés précédemment exposée, il suffirait de pousser le calcul jusqu'à $h = 154$ (*) exclusivement, c'est-à-dire qu'il y aurait seulement six valeurs à construire, sous le signe, dans l'expression de t, avec la condition de vérifier qu'il ne se trouve aucun carré parmi ces nombres (**).

Mais les formes, assignées aux valeurs de h, peuvent servir à abréger encore le calcul. En effet, la substitution des valeurs $90l + 24$, 28, 64, 78, dans l'expression de h, donnera les quatre formules suivantes

$$l = \frac{558\,634 - t(1525 - t)}{5580\,t + 90}, \qquad l = \frac{558\,630 - t(1773 - t)}{5580\,t + 90},$$

$$l = \frac{558\,594 - t(4005 - t)}{5580\,t + 90}, \qquad l = \frac{558\,580 - t(4873 - t)}{5580\,t + 90}.$$

Dans ces quatre valeurs, pour $t = 80$, l est moindre que 1. Mais, puisque t ne saurait atteindre 748, attendu que, si N n'est pas *premier*, son plus petit facteur simple $62t + 1$ ne peut se trouver au delà de la racine de N, et, par conséquent, au delà de 46341; puisque, en deçà de cette limite de 748, le dividende diminue (***) sans devenir nul (****), tandis que le diviseur augmente; il faut en conclure que l'hypothèse de $l = 0$ ne peut avoir lieu, et, en même temps, qu'il n'y a aucun essai à faire au delà de $t = 80$.

(*) Pour $h = 154$, t est moindre que 60.

(**) Il suffirait de former les six nombres

10121, 101001, 1533961, 2390201, 5360761, 5759161.

Aucun de ces nombres n'est un carré. (Voir la note seconde, page 15.)

(***) Le dividende diminue, puisque les produits de la forme $t(a - t)$ augmentent jusqu'à $t = \frac{a}{2}$, et que 748 est inférieur à cette limite dans les quatre formules.

(****) Pour s'assurer que le dividende ne devient pas nul, bien qu'il change de signe, il suffit de l'égaler à zéro et de résoudre l'équation. Cela revient du reste à vérifier qu'aucun des quatre nombres correspondant à $l = 0$ n'est un carré.

Si l'on fait $t = 60$, le quotient est compris entre 2 et 1 pour les deux premières valeurs de l, il est moindre que 1 pour les deux autres, de sorte qu'à employer la méthode des carrés, il y aurait seulement à vérifier les deux nombres qui correspondent à $h = 114$, et à $h = 118$ (*). Mais, si on veut se passer de la méthode des carrés, il s'agira de restreindre le nombre des essais de $t = 60$ à $t = 80$ (**). Or, si on pose $t = 70$ dans les deux premières formules, on trouve que le quotient est encore compris entre 2 et 1. Ainsi, les essais devraient se faire, dans les deux premières valeurs de l, de $t = 70$ à $t = 80$, parce que cet intervalle peut comprendre $l = 1$. Mais, entre ces deux limites, il ne se trouve, dans la suite que nous avons donnée, aucune valeur de t. On voit donc que l'hypothèse de $l = 1$, est inadmissible aussi bien que celle de $l = 0$. On pourrait encore simplifier les divers essais de $t = 0$ à $t = 60$ exclusivement, mais ces essais ne comprennent en définitive que douze opérations faciles à effectuer, à l'aide de la formule $h = \frac{558\,658 - t(37 - t)}{62t + 1}$, et les résultats s'obtiennent d'ailleurs avec une rapidité suffisante (***). Nous supprimons, bien entendu, les trois termes 8, 29 et 36.

Dans l'application que nous venons de faire de quelques principes nouveaux à la vérification du nombre *premier* N, le plus grand qui ait encore été vérifié, nous avons cherché à donner une idée des procédés qui peuvent être employés là où manquent les tables (****), et où viennent échouer, par la longueur des calculs, toutes les méthodes proposées jusqu'ici. Nos procédés, qui sont purement arithmétiques, exigent seule-

---

(*) Ces deux nombres sont 5360761, 5759161, dont aucun n'est carré. (Voir la note seconde, page 15.)

(**) Les seules valeurs de t à essayer seraient 65 et 68, parce que 69 donne un multiple de 11 pour $62t + 1$.

(***) Voir la note troisième, page 16.

(****) Les tables les plus étendues vont jusqu'à 4 000 000. Nous reconnaissons leur utilité; mais elles ont un inconvénient grave, c'est de laisser le plus souvent l'opérateur dans l'incertitude, par l'impossibilité où il est de vérifier rapidement d'aussi grands travaux.

ment qu'on soit parvenu à assigner une première forme aux diviseurs des nombres que l'on considère. Leur mérite est non-seulement de diminuer le nombre des essais, mais encore de remplacer les grands nombres sur lesquels il faudrait opérer, par d'autres beaucoup moins considérables. Du reste, nous nous proposons de revenir (*) sur cette belle question qui domine toute la théorie des nombres, ainsi que l'ont bien compris les grands géomètres qui n'ont pas dédaigné d'appliquer leur génie à cette partie difficile et ingrate de la science.

(*) L'un de nos plus prochains mémoires sera un essai de méthode générale.

NOTES DU SEPTIÈME MÉMOIRE.

NOTE PREMIÈRE,

Annoncée page 5.

Pour la première forme $248x + 1$, les multiples de 3 ou de 5 qu'il s'agit de retirer de la liste, correspondent aux valeurs de x comprises dans les formules

$$15a + 1, 3, 4, 7, 8, 10, \text{ et } 13,$$

jusqu'à $x = 186$. On pourra donc faire varier a depuis zéro jusqu'à 12; mais, pour $a = 12$, on ne devra prendre que les trois premiers termes $15a + 1, 3, 4$. On a en effet $180 = 15.12$; et, comme on ne doit pas dépasser 186, le dernier terme sera $15.12 + 4$. Ainsi il y aura 87 multiples de 3 ou de 5 jusqu'à cette limite.

Pour la seconde forme $248x + 63$, les multiples sont donnés par les valeurs de x comprises dans les formules

$$15a + 0, 3, 4, 6, 9, 12, \text{ et } 14,$$

depuis $a = 0$ jusqu'à $a = 12$, avec le soin de ne prendre, pour cette dernière valeur de a, que les quatre premiers termes

$$15a + 0, 3, 4, \text{ et } 6.$$

Il y aura donc 88 multiples, et par conséquent, pour les deux formes, le nombre des multiples de 3 ou de 5 sera 175.

NOTE SECONDE,

Annoncée page 8.

Ce tableau contient 28 nombres dont aucun n'est un carré. En voici le dépouillement :

Les nombres 101001, 17630601, 37833081, 959553 21, 112855161, 119093001 sont des multiples de 3, sans être divisibles par 9.

Les nombres 5360761, 18336521, 47569081, 97583801, 155877001, 163191161 sont des multiples de 7, sans être divisibles par le carré de 7.

Les nombres 1533961, 2390201 sont des multiples de 11, sans être divisibles par le carré de 11.

Pour les autres on a

1° $10121 = 100 . 100 + 121$; $5759161 = 2399 . 2399 + 3960$;
$9959801 = 3155 . 3155 + 5776$; $11892361 = 3448 . 3448 + 3657$;
$36819641 = 6067 . 6067 + 11152$; $62927881 = 7932 . 7932 + 11257$;
$64248841 = 8015 . 8015 + 8616$; $76752521 = 8760 . 8760 + 14921$;
$81914041 = 9050 . 9050 + 11541$; $135901961 = 11657 . 11657 + 16312$.

2° $25304841 = 9 . 2811649$ et $2811649 = 1676 . 1676 + 2673$;
$28313721 = 9 . 3145969$ et $3145969 = 1773 . 1773 + 2440$;
$51654281 = 49 . 1054169$ et $1054169 = 1026 . 1026 + 1493$;
$137837961 = 9 . 15315329$ et $15315329 = 3913 . 3913 + 3760$.

A ce sujet nous croyons devoir rappeler quelques principes :

1° Aucun nombre n'est carré s'il n'a l'une des terminaisons suivantes :

00, 01, 04, 09, 16, 21, 24, 25, 29, 36, 41, 44, 49, 56, 61,
64, 69, 76, 81, 84, 89, 96.

2° Tout nombre, qui contient un facteur *premier*, doit, s'il est carré, être divisible par une puissance paire de ce facteur.

3° Tout carré, qui n'a pas pour racine un nombre *premier*, doit contenir un facteur simple inférieur ou au plus égal à sa racine quatrième.

NOTE TROISIÈME,

Annoncée page 12.

Essai des nombres 5, 9, 20, 21, 24, 33, 41, 44, 45, 48, 53, 56 dans la valeur

$$h = \frac{558658 - t\,(37 - t)}{62\,t + 1}.$$

$t = 5$,	$558498 = 311 . 1795 + 253$;
$t = 9$,	$558406 = 559 . 998 + 524$;
$t = 20$,	$558318 = 1241 . 449 + 1109$;
$t = 21$,	$558322 = 1303 . 428 + 638$;
$t = 24$,	$558346 = 1489 . 374 + 1460$;
$t = 33$,	$558526 = 2047 . 272 + 1742$;
$t = 41$,	$558822 = 2543 . 219 + 1905$;
$t = 44$,	$558966 = 2729 . 204 + 2250$;
$t = 45$,	$559018 = 2791 . 200 + 818$;
$t = 48$,	$559186 = 2977 . 187 + 2487$;
$t = 53$,	$559506 = 3287 . 170 + 716$;
$t = 56$,	$559722 = 3473 . 161 + 569$.

Paris. — Typographie de Firmin Didot frères, fils et Cᵉ, rue Jacob, 56.